Status: September 2018

Sample design for a Law enforcement data protection act (Transposition of EU Directive 2016/680)[1]

Section 1
General provisions

Section 2
Collection

Section 3
Storage and use, file management

[1] The Schleswig-Holstein law enforcement data protection act served as a template, announced as Article 2 of the law on the enforcement of a sentence in Schleswig-Holstein and the creation of a law enforcement data protection act of July 21, 2016 (GVOBl. P. 618, 644).

Section 4
Transfer

Section 5
Special forms of data processing

Section 6
Protection requirements

Section 7
Special provisions for people with access to secret information

Section 8
Rights of the data subjects

Section 9
Deletion, limitation of processing and rectification

Section 10
Application of other provisions and final provisions

Article 1 General provisions

§ 1 Scope of application

(1) This Act regulates the processing of personal data by law enforcement authorities in the enforcement of

1. Imprisonment, youth punishment, detention, criminal arrest, lodging in the preventive detention, juvenile detention and
2. Detention pursuant to Article 127b, paragraph 2, Article 230, paragraph 2, Articles 236, 329, paragraph 3, Article 412, sentence 1, and Article 453c of the Code of Criminal Procedure, as well as temporary detention in accordance with Article 275a paragraph 6 of the Code of Criminal Procedure.

(2) Law enforcement authorities are correctional facilities, youth(criminal) institutions, juvenile detention institutions and facilities for the implementation of preventive detention (institutions), as well as for the ministry responsible for law enforcement (competent authority).

Article 2 Definitions

For the purposes of this law:

1."Prisoners" are persons in the penal system in accordance with Article 1 paragraph 1;
2. "Law enforcement purposes"
   a) to empower the prisoners to lead a life without crime in the future with social responsibility,
   b) to protect the public from further criminal offenses of the prisoners
   c) to protect body, life, freedom, and property of staff and prisoners, as well as the assets of the country by the maintenance of security and order within the institutions,
   d) to prevent escape and liberation of prisoners,
   e) to avoid non-return and abuse of the relaxations as well as
   f) the involvement of the law enforcement in the other tasks entrusted to it by law, and in particular with preparatory opinions about the decisions of the criminal enforcement chambers which relate to prisoners;

the place of the particular purpose in paragraph 2(a) shall enter into force for the implementation of pre-trial detention, by the safe storage of prisoners in order to ensure the implementation of ordered criminal proceedings;

3. "Personal Data" means any information relating to an identified or identifiable natural person (person); a natural person is considered to be identifiable, if they can be identified directly or indirectly, in particular by means of assignment to an identifier such as a name, an identification number, location data, an online ID or to one or more specific characteristics, the expression of the physical, physiological, genetical, mental, economic, cultural or social identity of this person;
4. "Processing" means any procedure carried out with or without the help of automated methods or any such series of procedures in connection with personal data such as
   a) the collection, recording, storage, modification, reading, consultation, disclosure by transmission, dissemination or any other form of deployment, the comparison, deletion, restriction or destruction or
   b) the organization, arranging, adaptation, the linking or for any other use (use);
5. "Limitation of processing" means the marking of stored personal data with the aim of limiting its processing in the future;
6. "Profiling" means any kind of automated processing of personal data which involves the use of such personal data to evaluate certain personal aspects relating to a natural person, particularly to analyse or predict aspects relating to job performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or change of location of this natural person;
7. "Pseudonymization" is the processing of personal data in a manner in which the data, without additional information, cannot be assigned to a specific data subject, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the data cannot be assigned to any data subject;
8. "Anonymization": the changing of personal data in such a way that the individual details about personal or factual circumstances can no longer be assigned to a specific or identifiable natural person, or only with a disproportionately large amount of time, cost and labour;
9. "File system" means any structured set of personal data which is accessible according to specific criteria, independently of the fact whether this set is managed on a centralized or decentralized basis, or it is organized on a functional or geographical basis;

10. "Manager" means a natural or legal person, public authority, agency or other body which alone or jointly with others makes decisions about the purposes and means of the processing of personal data;
11. "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the manager;
12. "Recipient" means any natural or legal person, public authority, agency or other body to whom the personal data is disclosed, regardless of whether it is a third party or not; those authorities shall not be considered as recipients who, in the context of a specific investigation order, in accordance with Union law or other legislation, obtain personal data; the processing of this data by the authorities referred to shall be carried out in accordance with the applicable data protection regulations in accordance with the purposes of the processing;
13. "Personal data breach" is a breach of security involving the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to personal data that has been processed;
14. "Special Categories of Personal Data"
    a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership,
    b) genetic data,
    c) biometric data for the unique identification of a natural person,
    d) health data and
    e) data on sex life or sexual orientation;
15. "Genetic data" is personal data on the inherited or acquired genetic properties of a natural person, that give unique information about the physiology or the health of this person, in particular those that were gained from the analysis of a biological sample of the person;
16. "Biometric data": personal data gained with special technical processes, relating to the physical, physiological or behavioural characteristics of a natural person, or allowing or confirming the unambiguous identification of this natural person, especially facial images or dactyloscopic data;
17. "Health information" is personal data relating to the physical or mental health of a natural person, including the provision of health services, and data from which information about their state of health can be deduced;
18. "International organization" means an international organization and its subordinate agencies, and any other entity created by or based on an agreement concluded by two or more States;
19. "Consent": any declaration of intention for the particular case, in any informed and unequivocal way, in the form of a declaration or any other unique affirmative

action, with which the data subject expresses that they allow the processing of the given personal data;

20. "Persons outside the institution" means persons who are not in a service or employment relationship with the prison authorities, and do not act on behalf of any other authority, or do not act as an administration of justice body.
21. "Public Bodies"
    a) the authorities, the organs of administration of justice and other institutions organized under public law of the Federation, the federal bodies, the institutions and foundations of public law and their associations, irrespective of their legal form,
    b) the authorities, the organs of administration of justice and other institutions organized under public law of a country, community, association of municipalities or other public law entities subject to supervision of the country and their associations, irrespective of their legal form and;
    c) the authorities, the organs of administration of justice and other institutions organized under public law of a Member State of the European Union;

22. "Non-public bodies" means natural and legal persons, companies and other associations of persons governed by private law, other than those subject to Point 21; if a non-public body performs public administrative tasks, it is a public body according to this law.

Article 3 Principles of data processing

(1) Law enforcement protects the right of every person to decide, in principle, about the disclosure and use of their personal data.

(2) Data processing must be oriented towards processing as little personal data as possible. The possibilities of anonymization and pseudonymization shall be used as far as this is possible according to the purpose of the processing.

(3) As far as possible, the processing of personal data should be distinguished according to whether it is based on facts or on personal assessments.

(4) A decision based solely on the automated processing of personal data, which has a negative legal consequence on the data subjects or significantly affects them, is inadmissible. Profiling that entails that the data subjects are discriminated against based on special categories of personal data is prohibited.

Article 4 Admissibility of data processing, consent

(1) The law enforcement authorities may only process personal data if this law or any other legislation relevant to the scope of this law expressly allows or orders it, or the data subjects have given their consent and the consent does not preclude a statutory ban.

(2) If the processing of personal data takes place based on consent, the law enforcement authority must be able to prove the consent of the data subjects.

(3) If the data subject's consent is provided by a written statement also concerning other matters, the request for consent must be made in a clear and accessible manner in clear and simple language, so that it is clearly distinguishable from the other matters.

(4) The data subjects have the right to revoke their consent at any time. The revocation of consent does not affect the legality of the processing carried out based on the consent until the revocation. The data subjects shall be informed prior to the transfer of the consent.

(5) The consent is only effective if it is based on the free choice of the data subjects. In assessing whether the consent was given voluntarily, the circumstances of the issuance, for example, the special situation of deprivation of freedom, are to be taken into account. The data subjects are to be informed about the purpose of the processing. If it is required due to the circumstances of the individual case or if the persons concerned request this, they must also be informed of the consequences of refusing consent.

(6) As far as special categories of personal data are to be processed, the consent must expressly relate to this data.

(7) For prisoners with limited legal capacity, the ability to consent is determined by the actual cognitive ability.

(8) If the prisoners do not have the necessary cognitive ability to make a decision, and if this does not endanger the enforcement purposes, their rights under this law to

be informed and to be asked or to ask questions and make requests shall be assigned to their legal representatives. When several persons are entitled, each of them can exercise certain rights determined in this law alone. If communications are required, it is sufficient if they are addressed to one of them.

Article 5 Data secrecy

(1) The persons engaged in law enforcement must not process personal data without authorization (data secrecy). Persons who are not officials within the meaning of Article 11 paragraph 1 (2) of the Criminal Code, shall be informed about the provisions to be observed before taking up their duties, and they shall be obliged to comply with those in accordance with Article 1 of the BGBI law of March 2, 1974 (BGBl. I S. 469, 547), which is modified by Article 1(4) of the law of August 15, 1974 (BGBl. I S. 1942), in the respective valid version.

(2) The confidentiality of data persists even after completion of the work.

Section 2 Collection

Article 6 Admissibility of data collection

(1) Law enforcement authorities may collect personal data, if it is necessary for law enforcement purposes.

(2) Special categories of personal data may only be collected if this is absolutely necessary for law enforcement purposes.

Article 7 Collection from data subjects

(1) Personal data is generally collected from the data subjects and with their knowledge.

(2) The collection of personal data of the data subjects without their knowledge is permitted if there is no indication that the legitimate specific interests of the data subjects are affected.

Article 8 Collection of data on prisoners from third parties

(1) If the collection of personal data on prisoners is permitted in accordance with Articles 6 and 7 paragraph 2, they may also be collected from third parties without the knowledge of the prisoners, if

1. this is required in order to achieve the enforcement goal or to prevent imminent danger to the safety of the institution,
2. this is expressly permitted or ordered by legislation,
3. data of the data subjects must be checked because there are actual indications of their incorrectness,
4. this is required to prevent significant disadvantages for the common good or an otherwise imminent danger to public safety,
5. this is required to prevent serious impairment of the rights of another person,
6. the collection relates to data from documents of the judicial proceedings which underlie the execution of the present deprivation of liberty or otherwise affect this deprivation of liberty,
7. the data subjects have not complied with an obligation laid down by legislation to provide information and they have been informed about the intended collection from third parties,
8. the collection from the data subjects would require a disproportionate effort or
9. the data is generally accessible.

(2) If the collection of personal data about prisoners is permitted in accordance with Articles 6 and 7 paragraph 2, and they do not possess the necessary insight for their consent, personal data may also be collected from their legal representatives without their knowledge.

(3) Non-public bodies are obliged by the legal provision which obliges them to inform, otherwise to the voluntariness of their information.

Article 9: Collection of data on persons who are not prisoners

(1) Data on persons who are not prisoners can be collected without their knowledge from prisoners or other third parties, as far as this is strictly necessary for enforceable

purposes and protection-worthy interests of the data subjects are not thereby impaired.

(2) Non-public bodies are obliged by the legal provision which obliges them to inform, otherwise to the voluntariness of their information.

Section 3 Storage and use, file management

Article 10 Storage and use

(1) The law enforcement authorities may store and use personal data that have been collected in a permitted way, if this is necessary for enforcement purposes.

(2) The law enforcement authorities may only use and store personal data that have been collected in a permitted way for purposes other than for which the data was collected, if

1. the prerequisites exist that permit the collection of data from third parties pursuant to Articles 8 or 9; if prisoners other than those whose deprivation of liberty was the original cause of the collection are affected by other processing, then the personal data may only be stored or used for a different purpose, if these prisoners have been heard previously with specifying the intended data processing, and there is no interest predominantly worthy of protection to exclude the processing of personal data concerning them,
2. this is expressly permitted or ordered by legislation,
3. it serves judicial protection, the exercise of supervisory and controlling powers, the automation of reporting, auditing, the implementation of organizational investigations or statistical purposes of the law enforcement authorities, and does not conflict with the protection-worthy interests of the data subjects,
4. this is necessary for the defence against security-endangering or secret service activities for a foreign power or efforts in the Federal Republic of Germany, using force or preparatory acts
   a) that are directed against the free democratic basic order, the existence or the security of the Federation or a region,
   b) the purpose of which is to have an illegal effect on the administration of the constitutional organs of the Federation or of a region or its members or
   c) endangering the foreign interests of the Federal Republic of Germany,

5. this is required to avert significant disadvantages for the common good or a danger to public security,
6. this is required in order to prevent serious impairment of the rights of another person,
7. this is necessary for the prevention or prosecution of criminal offenses, for the enforcement of penalties and measures within the meaning of Article 11, paragraph 1, point 8, of the Criminal Code, as well as for the prevention or prosecution of offenses through which the security or public order of the institution is at risk or
8. this is required for criminal enforcement measures or criminal enforcement legal decisions regarding the data subjects.

(3) Storing or using legally collected special categories of personal data for purposes for which they were not collected, is only permitted if it is absolutely necessary for the purposes referred to in paragraph 2. If the special categories of personal data collected are subject to official or professional secrecy, and have been obtained from the persons subject to secrecy in the exercise of their official or professional duties, they may be stored or used only for the purpose, for which the persons obliged to secrecy have received them, unless otherwise provided by this law.

(4) Personal data that have been collected in accordance with Article 9 on persons who are not prisoners may only be stored and used under the conditions set out in paragraph 1 or paragraph 2, point 2, 4 to 6, under the conditions laid down in Article 16 or for the prevention or prosecution of criminal offenses of considerable importance.

(5) If personal data that may be processed in accordance with paragraph 1 or paragraph 2 involves further personal data of data subjects or of third parties in files in such a way that separation is not possible or only with unreasonable effort, the storage of this data is also permissible if the legitimate interests of data subjects or third parties evidently outweigh this secrecy. Use of these data is not permitted.

(6) Personal data that are stored or used solely for the purposes of data protection control, data backup or to ensure the proper operation of a data processing system, may only be used for other purposes if this serves to avert a significant risk to public safety, especially for life, health or freedom, as well as to prosecute crimes of significant importance. The further processing of log data shall be governed by Article 42 paragraph 3.

Article 11 File management

(1) Prisoner's personal files and health records must be kept.

(2) The law enforcement authorities may also manage files electronically. The ministry responsible for law enforcement is authorized to designate arrangements for the electronic management of files by legal regulation.

Section 4 Transfer

Article 12 Transfer to public and non-public bodies

(1) The law enforcement authorities may transfer personal data that they have collected legally to the extent necessary for law enforcement purposes.

(2) Non-governmental organizations may transfer the personal data collected to the law enforcement authorities for purposes for which they were collected, as far as

1. the law enforcement authorities make allowable use of non-public bodies for the purpose of achieving individual, enforceable functions and that such cooperation would be impossible or significantly more difficult without the processing of personal data transmitted by law enforcement authorities; and
2. it is necessary to make possible for prisoners
   a) visits from treatment, consulting, training and education measures as well as the employment within and outside the institutions,
   b) the use of the services of the professional and secrecy holders (§ 45 (2)) and their assistants,
   c) the purchase or
   d) the use of telecommunications and media services,
   e) the use of measures of discharge preparation, the transition into freedom, debt settlement, dismissal, reintegration, aftercare or voluntary retention

.

(3) Competent public organizations may transfer legally collected personal data to the law enforcement authorities for purposes for which they were not collected, as far as

1. any other legal provision expressly permits or orders it for the scope of this law or

2. this is necessary for
   a) the fulfilment of the duties of judicial assistance, juvenile court help, probation service, management supervision or forensic ambulances,
   b) decisions in pardons,
   c) statutory statistics of justice,
   d) the performance of tasks transferred to the competent service providers by legislation,
   e) the introduction of aid measures for relatives of the prisoners (Article 11 paragraph 1 point (1) of the Criminal Code),
   f) official measures of the Federal Army in connection with the admission and discharge of the soldiers,
   g) asylum or foreigner law measures,
   h) the fulfilment of the tasks of the youth welfare offices,
   i) the implementation of taxation or
   j) the achievement of the objectives set out in Article 10, paragraph 2, point 2 to 8 or Article 16.

(4) in the implementation of pre-trial detention and deprivation of freedom in accordance with § 1 paragraph 1 point 2 transfers referred to in paragraph 3, point 2 may be omitted if the prisoners, taking into account the nature of the information and their legal status, have a legitimate interest in the exclusion of transfer.

(5) In the absence of consent of the data subjects, the non-public authorities may only transfer the collected personal data to the law enforcement authorities for purposes for which the data were not collected under the conditions of Article 10 paragraph 2 point 2 to 8.

(6) The transfer of special categories of personal data collected may be allowed
1. to public authorities only under the conditions laid down in Article 10, paragraph 3, Articles 16 and 28,
2. to non-public bodies only under the conditions that it is strictly necessary and
   a) a piece of legislation expressly permits or orders this, for the scope of this law,
   b) this serves the fulfilment of law enforcement purposes,
   c) This also considers the interests of the prisoners in the confidentiality of personal data
      (aa) this serves as defence against a threat to the life of a person, especially for the prevention of suicides,

(bb) this serves to avert a serious threat to the health or other vital interests of a person or

(cc) this serves to avert the risk of serious criminal offenses,

d) this is required to avert significant disadvantages for the common good or otherwise imminent threats to public security,

e) the data of the data subjects was obviously made public.

3. to forensic clinics for the purpose of treatment measures, discharge preparation and aftercare, as far as this is strictly necessary,

.

(7) Personal data which are collected in accordance with Article 9 on persons who are not prisoners, may only be used under the conditions set out in paragraph 1 or for the purpose set out in Article 10 paragraph 2 points 4 to 6 or article 16 as well as for the prevention or prosecution of criminal offenses of considerable importance. They may also be transferred if it is necessary for purposes of investigation and arrest of escaped prisoners or prisoners who are outside the institution without permission.

(8) If personal data that may be transferred in accordance with paragraphs 1, 3 or 4 is associated with other personal data of data subjects or third parties in files in such a way that separation, anonymization or pseudonymization is not possible or only possible with unreasonable effort, then the transmission of these data is also permitted, as far as legitimate interests of data subjects or third parties obviously outweigh their secrecy. As far as special categories of personal data are concerned, it is to be assumed that the data subjects have a predominantly legitimate interest. Storage use and transmission of this data by the recipient is not permitted.

(9) Unless otherwise specified, the transmission of personal data does not take place if the personal data

1. have become known to the law enforcement authorities from people holding secrets within the meaning of Article 45 paragraph 1; or
2. are restricted or incorrect in their processing.

Article 13 Safety-relevant findings

(1) For the purpose of maintaining the safety of the institution, law enforcement authorities shall examine, in accordance with the provisions of Articles 14 and 15, whether there is safety-relevant knowledge about prisoners and non-institutional people who want access to the prison institutions.

(2) A safety-relevant finding is knowledge particularly about extremist, violence-oriented orientation or contacts with such organizations, groups or persons or contacts to organized crime. If non-institutional people work on the reintegration of prisoners, under sentence 1, knowledge about significant criminal convictions, an existing addiction or other significant circumstances relevant for the assessment of reliability can be safety relevant.

Article 14 Prisoner review

(1) If there is any real evidence of imminent danger to the safety of the institution ascribable to a prisoner, the law enforcement authorities may ask the judicial and security authorities for information. For that purpose, they may, in particular:

1. information in accordance with Article 41 paragraph 1 point 1 of the Federal Central Criminal Register Act in the version promulgated on September 21, 1984 (BGBl. p. 1229, 1985, p. 195), the last by the law of July 18, 2017 (BGBl. p. 2732) has been modified in the up-to-date version,
2. inquire about safety-relevant findings of the police authorities of the Federation and the regions and,
3. If necessary, in each individual case, they may inquire about safety-relevant findings of the State Office for the protection of the Constitution.

The real evidence of imminent danger to the safety of the institution ascribable to a prisoner, can come from the sentence of the prisoners or their behaviour in enforcement.

(2) The request referred to in paragraph 1, sentence 2 point 2 extends only to the personal indications and the findings of the police state security. In the request referred to in paragraph 1, sentence 2 point 3, the request of the intelligence information system is made by the State Office for the protection of the Constitution.

(3) The law enforcement authorities shall provide the requested authorities, with the last name, birth name, first name, date of birth, gender, place of birth, country of birth and nationality of the prisoners, if possible. In terms of sentence 1, the also known personal data, the estimated time spent under enforcement, as well as the file number underlying the enforcement decision should be provided.

(4) The authorities requested in accordance with paragraph 1, sentence 1 and sentence 2 point 2 and 3 shall notify the law enforcement authorities of safety-relevant knowledge about the prisoners.

(5) If, based on the transferred safety-relevant insights, there is actual evidence of a threat to the security of the institution, the law enforcement authorities may request additional information or documents from judicial and security authorities.

(6) The security relevant findings that were shared in the context of the request, shall be kept in separate files or file systems.

(7) The authority for processing and transmission of personal data on prisoners to maintain the security of the institute includes the authority to process for the purpose of law enforcement and integration planning of the prisoners.

Article 15 Review of non-institutional persons

(1) Non-institutional persons who are to work in the prison may only be admitted to these activities if there are no safety concerns. The law enforcement authorities shall perform a background check with consent of the data subjects in order to maintain the security of the institution. For that purpose, they may, in particular:

1. request Information in accordance with Article 41 paragraph 1 point 1 of the Federal Central Criminal Register Act,
2. inquire about safety-relevant findings of the police authorities of the Federation and the regions and,
3. if necessary, in each individual case, they may inquire about safety-relevant findings of the State Office for the protection of the Constitution.

If a check is not possible in urgent cases, especially in the event of short-term repair work, supervision of persons during their work in the prison should take place.

(2) The law enforcement authorities should refrain from requesting the third sentence of paragraph 1 if there is no risk to the safety of the institution as a result of the occasion, nature, scope or duration of their stay or activity in the institution.

(3) In addition, the prison authorities may do a background check if there are actual indications of an impending danger to the security of the institution, even about persons asking for the admission to visit prisoners or to visit the institution, with their consent. Paragraph 1, sentence 3 shall apply accordingly. In the cases referred to in paragraph 1, sentence 3 number 2 and 3, the law enforcement authorities also share whether the permission to visit is requested and for which prisoners.

(4) Paragraph 3 shall not apply to visits by defence counsels and legal assistants, lawyers and notaries in a case concerning the prisoners, and to persons and bodies privileged by law in the context of monitoring prisoners' written correspondence.

(5) If the law enforcement authorities become aware of safety-relevant findings, the persons not belonging to the institution should not be admitted or only admitted to the activity or visit with restrictions. The same applies if the data subjects reject a background check.

(6) a new background check should be done if there are new safety-relevant findings in accordance with Article 13 paragraph 2, at the latest, however, after the expiration of five years, unless their necessity pursuant to paragraph 1, sentences 1 and 2 and paragraph 3 persists.

Article 16 Case conferences

(1) In case conferences, the law enforcement agencies may transmit personal data, including those of special categories which they have collected in an admissible way, in particular the anticipated dismissal date, probable discharge address and enforcement and integration plans, federal and state police authorities, provided that the following exist:

1. actual evidence of the continuing danger of prisoners for the community,
2. the release of prisoners, in all probability, in a period of not more than one year and
3. this is necessary for the prevention of illegal acts that are of considerable importance.

Case conferences may also be held to prepare for performance, demonstration, cancellation, transfer and relocation of actual evidence of danger of escape, acts of violence against persons or objects of significant value the conservation of which is necessary in the public interest, and the danger of self-harm or suicide of prisoners. The probation service and the management supervisory agencies should be involved in case conferences referred to in sentence 1. In the case conferences referred to in sentences 1 and 2, the law enforcement authorities may also query and collect personal data from the police authorities, including such special categories.

(2) In case conferences, the law enforcement authorities may transmit personal data to the constitutional protection authorities of the federation or the states, including data of special categories which they have collected in an admissible way, in particular the anticipated dismissal date, probable discharge address and enforcement and integration plans, provided that the following exist:

1. certain facts establish the suspicion about activities or efforts in accordance with Article 10, paragraph 2, point 4,
2. a threat associated with it that endangers the security of the institution or the achievement of the enforcement purpose in a reasonable period of time and
3. this is absolutely necessary for the prevention of risks referred to in point 2.

The probation service and the management supervisory agencies should be involved in the case conferences, provided the release of the prisoners is expected to take place in less than a year. In the course of these case conferences, the law enforcement authorities may also query and collect personal data, including those of special categories, from the constitutional protection authorities of the Federation and the regions.

(3) Case conferences may take place between the law enforcement authorities, the police authorities of the Federation and the regions and the constitutional protection authorities of the Federation and the regions, if

1. certain facts justify the assumption of a present danger to life and body, health or freedom of a person or of objects of considerable value, whose preservation is necessary in the public interest,
2. certain facts justify the assumption of activities or efforts in accordance with Article 10, paragraph 2, point 4, and
3. this is absolutely necessary for the prevention of risks referred to in point 1.

Paragraph 2 sentence 2 shall apply accordingly. In the course of these case conferences, the law enforcement authorities may also query and collect personal data from the police authorities of the Federation and the regions as well as the

constitutional protection authorities of the Federation and the regions, including data of special categories.

(4) The main results of the case conferences are to be documented.

(5) The enforcement and integration planning belong to the law enforcement authorities.

Article 17 Other admissibility requirements for data processing with the safety authorities

(1) The transfer of personal data to security authorities for the purpose of risk prevention, for purposes of danger prevention, for the prevention or prosecution of criminal offenses, for the prevention or prosecution of offenses or for purposes mentioned in Article 10 paragraph 2 number 4 is only permitted if

1. there are concrete approaches in individual cases
   a) for the prevention, detection or prosecution of criminal offenses or offences, or
   b) to ward off dangers threating in a reasonable period of time
   and
2. at least
   a) the protection of such important legal interests or
   b) the prevention, detection or prosecution of serious criminal offences or offences is to be realized,

so that the protection of legal rights is ensured that is of the same value as data collection.

(2) Paragraph 1 shall apply to the collection of personal data by the law enforcement authorities from the security authorities on prisoners, non-institutional or other persons for the purpose of risk prevention, prevention or prosecution of criminal offenses or for the prevention or prosecution of offenses accordingly.

(3) For the transfer and collection of personal data that were obtained by the hidden use of technical means to or from homes, or covert intervention in information technology systems, the provisions of paragraph 1 point 1 (b) applies provided that

1. in the case of personal data obtained by the hidden use of technical means to or from homes, on a case-by-case basis, there must be urgent danger for the inventory or the security of the Federation or a region or a risk to life, limb or liberty

of a person or property of significant value, whose preservation is necessary in the public interest, and

2. in the case of personal data obtained through a covert intervention in information technology systems, in individual cases certain facts justify the assumption in any case that damage to the life, limb or freedom of a person or such goods happens within a manageable period of time in a way concretized at least in its own way whose threat affects the foundations or the existence of the state or of a country, or the foundations of human existence.

(4) the power to detect official comparison of data for the purposes of identification of prisoners (Article 28) and non-institutional persons (Article 35 paragraph 4) remains unaffected.

Article 18 Responsibility for the transfer of data and procedures

(1) The responsibility for the permissibility of the transfer lies with the transmitting law enforcement authority.

(2) If the transfer is carried out at the request of a public body, this public body shall bear the responsibility. In that case, the law enforcement authorities shall only check whether the request is within the remit of the receiving public authority and this law does not preclude the transfer, unless there is a reason to examine the admissibility of the transfer.

(3) If the transfer is made at the request of a non-public authority, the latter must provide the information necessary for this, in particular the legal basis for the transmission.

(4) Insofar as this is possible with reasonable time and effort, the personal data shall be checked for correctness, completeness and topicality before they are submitted.

(5) In the case of the transmission of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal sanctions including the protection from and the prevention of threats to public security, the necessary information shall be added as far as possible, which enables the receiving public authorities to check the correctness, completeness and reliability of the personal data as well as to assess the degree of being up-to-date

(6) Personal data to be transmitted to non-public authorities shall be pseudonymized prior to transfer, unless the personal reference is necessary for the fulfilment of the purpose of the transmission. The prisoner booking number shall be used as a pseudonym, unless there are special reasons against that.

Article 19 Formal obligation of third parties

(1) Persons who are to obtain knowledge of personal data for a non-public body which data have been transferred by law enforcement authorities, are to be formally obliged before commencing their activities in accordance with Article 1 of the Commitment Act, as amended.

(2) Persons who were not formally obliged according to paragraph 1 may only gain knowledge of personal data if

1. the transmitted data is pseudonymized before transmission,
2. the formal obligation before obtaining knowledge would jeopardize the life or limb of a person or significant assets and the obligation is arranged and made up for immediately; if the transmission of the data is not carried out by the law enforcement authorities, they must be informed of the transmission without delay, stating the personal details of the persons obtaining the knowledge; or
3. they are officials within the meaning of Article 11 paragraph 1 point 2 of the Criminal Code.

(3) The law enforcement authorities shall ensure in an appropriate manner, that in the case of non-public bodies only such persons gain knowledge of transferred personal data who had previously been obliged in accordance with paragraph 1 or who, under paragraph 2, may obtain information about personal data transferred, even without a formal obligation.

Article 20 Communication on prison conditions

(1) The law enforcement authorities may inform, at written request, whether a person is in prison and, if so, in which institution, whether their dismissal is anticipated within one year and, if the dismissal is within one year, the probable date of the dismissal, in so far as

1. the communication is required in order to fulfil the tasks that lie within the competence of the inquiring public body or
2. non-public organizations have a legitimate interest in this communication, and the prisoners concerned have no legitimate interest in the exclusion of transmission.

(2) The victims of a criminal offense and their legal successors may, in addition to paragraph 1, be provided with information, at written request, about

1. release address or the financial situation of prisoners, if the granting of information is necessary to determine or enforce legal claims in connection with the offense,
2. the granting of first relaxations, if they have a legitimate interest and there are no overriding protection-worthy interests of the prisoners on the exclusion of communication.
3. relaxations granted to the prisoners if a legitimate interest has been set out or is evident, and there is no overriding protection-worthy interest of the prisoner in the exclusion of the notification.

(3) In the cases referred to in paragraph 2 point 2, this requires the presentation of a legitimate interest, if the applicant is the victim of a criminal offence according to

1. Articles 174 to 182, 184i and 184j of the Criminal Code,
2. Articles 211 and 212 of the Criminal Code, which had been attempted,
3. Articles 221, 223 to 226 and 340 of the Criminal Code,
4. Articles 232 to 238, Article 239 paragraph 3 and Article 239a, 239b and Article 240 paragraph 4 of the Criminal Code or
5. Article 4 of the Violence Protection Act of December 11, 2001 (BGBl. p.3513)

. Sentence 1 shall apply mutatis mutandis in cases under Article 395 paragraph 3 of the Code of Criminal Procedure, if the applicant has been approved to incidental action.

(4) In addition to paragraph 1, competent public authorities may be provided with information about the discharge address or the financial circumstances of prisoners if

this is necessary to establish or enforce public-law claims.

(5) In the implementation of pre-trial detention and deprivation of freedom in accordance with Article 1 paragraph 1 point 2, the permissible communication referred to in paragraphs 1 and 2 shall indicate whether or not a person is in the institution in pre-trial detention or subject to deprivation of freedom. A transmission fails, if the prisoners, taking into account the nature of the information and their legal status, have a legitimate interest in the exclusion of transmission.

(6) The prisoners concerned will be heard prior to the communication, unless it can be expected that the interests of the applicant would be thwarted or materially complicated through that, and that such interests outweigh the interests of the prisoners in their previous hearing. If the hearing is omitted, the prisoners concerned are informed subsequently, stating the content of the communication.

7) In the event of hearing and informing prisoners in accordance with paragraph 6, the legitimate interests of non-public recipients in the secrecy of their living conditions shall be taken into account in a special way. The address of the recipient may not be delivered to the prisoners.

(8) Notifications are placed in the prisoner's personal files to document the prisoners concerned.

Article 21 File transfer

(1) Insofar as the transmission of the data contained therein is permitted, personal data files may only be transferred to

1. law enforcement authorities,
2. Court assistance, Juvenile court assistance, probation service or supervision of conduct,
3. courts competent in the sentence, criminal law enforcement and criminal decisions,
4. the criminal law enforcement and law enforcement authorities,
5. the judicial enforcement, law enforcement or criminal law enforcement authorities or bodies appointed by a court with opinions; and
6. other public authorities, if the granting of information would either require an unreasonable effort or after presentation of the information, the authority

requesting the communication of information does not have sufficient data for the performance of their duties,

or in the case of electronic records management in the form of duplicates.

(2) If personal data, that may be transmitted in accordance with Article 12, paragraphs 1, 3 or 5, is associated with other personal data of data subjects or third parties in files in such a way that separation, anonymization or pseudonymization is not possible or only possible with unreasonable effort, then the transmission of data is permitted under paragraph 1, as far as non-legitimate interests of data subjects or third parties obviously outweigh their secrecy. As far as special categories of personal data are concerned, it is to be assumed that the data subjects have a predominantly legitimate interest. The storage, use and transmission of further personal data by the receiving public authority pursuant to sentence 1 is not permitted.

Article 22 Information and inspection for scientific purposes

(1) The transfer of personal data in files to universities and other institutions that do scientific research, and to public bodies for scientific purposes shall be governed by Article 476 of the Code of Criminal Procedure in accordance with the requirement that electronically stored personal data can also be transferred. The transmission can also be carried out electronically.

(2) In the implementation of pre-trial detention and deprivation of freedom in accordance with Article 1 paragraph 1 point 2, transfers referred to in paragraph 1 are not conducted if it is apparent to the transmitting body that the prisoners, taking into account the nature of the information and their legal status, have a legitimate interest in the exclusion of transmission.

Article 23 Inspection of prisoner's personal records, health records and medical records

The members of a delegation from the European Committee for the prevention of torture and inhuman or degrading treatment or punishment to the institution will receive insight into the prisoner's personal records, health records and medical

records in the prison hospital during the visit, to the extent essential for the performance of the duties of the committee.

Section 5 Special forms of data processing

Article 24 Data processing on order

(1) The law enforcement authorities may let personal data be processed by other persons or bodies on order to. This also applies to test and release procedures, inspection and maintenance work and similar auxiliary activities, including remote maintenance.

(2) In the cases referred to in paragraph 1, the law enforcement authorities remain responsible for the compliance with the provisions of this act and any other applicable regulations regarding data protection. The rights of the data subjects to access, rectification, cancellation, restriction of the processing and compensation are to be claimed in this case vis-à-vis the law enforcement authorities.

(3) The law enforcement authorities may only commission such processors with the processing of personal data which ensure with appropriate technical and organizational measures that the processing is carried out in accordance with legal requirements and that the protection of the rights of data subjects is ensured.

(4) Processors may not use other processors without the prior written approval of the law enforcement authorities. Before any intended change in relation to the involvement or the replacement of other processors, the law enforcement authorities must be informed.

(5) If a processor adds another processor, he shall apply the same obligations under his contract with the law enforcement authorities under paragraph 6, which also apply to him, unless those obligations are already binding on the other processor by other provisions. If these obligations are not fulfilled by another processor, then the processor who assigned that processor shall be liable vis-à-vis the law enforcement authorities for the observance of the obligations of the other processor.

(6) Processing by a processor shall be on the basis of a written contract or other legal instrument binding the processor to the law enforcement authorities and determines

the subject, duration, nature and purpose of the processing, the nature of the personal data, defines the categories of data subjects and the rights and obligations of the law enforcement authorities. The contract or other legal instrument shall include, in particular, that the processor

1. only deals with documented instructions of law enforcement; if the processor is of the opinion that an instruction is illegal, he must inform the law enforcement authorities immediately,
2. ensures that persons authorized to processing of personal data are obliged to maintain confidentiality, in so far as they are not subject to any reasonable legal confidentiality obligation,
3. supports the law enforcement authorities with appropriate means to guarantee the compliance with the provisions on the rights of the data subjects,
4. returns or deletes and destroys existing copies of all personal data after the completion of the execution of the processing services at the choice of the law enforcement authorities if there is no obligation to store the data in accordance with a legislation;
5. provides the law enforcement authorities with all relevant information, in particular the reports created in accordance with Article 42, in order to prove compliance with its obligations,
6. allows and contributes to checks conducted by the law enforcement authorities or someone assigned for this purpose,
7. observes the conditions set out in paragraphs 4 and 5 for the use of the services of another processor,
8. makes all measures that are necessary in accordance with Article 40 and
9. supports the law enforcement authorities, taking into account the nature of the processing and the available information, in observance of the obligations referred to in Articles 40, 41 and 64 paragraph 1 point 1 and 5.

(7) A processor who determines the purposes and means of the processing in contravention of this provision shall be responsible in relation to this processing.

(8) Article 19 shall apply mutatis mutandis.

Section 25 Data Processing for the transfer of implementation tasks

(1) If tasks are transferred for enforcement purposes in a permissible manner to public or non-public offices for execution, personal data may be transmitted as far as

this is necessary for the performance of the tasks. Special categories of personal data may only be transferred if it is absolutely necessary for the fulfilment of the tasks. Where the transmission is permissible in accordance with sentences 1 or 2, files and file systems may be entrusted if it is necessary for the performance of the tasks.

(2) The contractor is to be selected carefully pursuant to paragraph 1, sentence 1. It must also be considered whether the contractors provide sufficient assurance that they are in a position to take the technical and organizational measures required for data protection-compliant data processing. The assignment shall be given in writing or in electronic format. It contains information on the subject matter and the scope of the delegation of tasks, the necessity of processing of personal data in order to fulfil delegated tasks and the formal commitment of personnel to be deployed for this purpose pursuant to section 1 of the commitment law in the respective valid version. The law enforcement authorities are obliged to regularly check and document compliance with the data protection measures taken by the contractors.

(3) If the contractor processes personal data for the fulfilment of the tasks assigned to them, the provisions of this law shall apply mutatis mutandis.

Article 26 Common responsibility of law enforcement authorities

If two or more law enforcement authorities jointly establish the purposes and means of the processing, they shall be deemed to be jointly responsible. They have their respective roles and responsibilities of data protection law in a transparent form in an agreement, as long as these are not already established in laws. In particular, the agreement must specify who has to fulfil which information obligations, and how and to whom data subjects can exercise their rights.

Article 27 Identification measures

(1) For law enforcement purposes, and in particular to establish the identity and security of the institution, the following are permissible with the knowledge of the prisoners:
1. the taking of photos,
2. the recording of finger and palm prints,

3. The determination of physical characteristics,
4. Measurements,
5. the collection of biometric characteristics of fingers, hands, face, eyes, voice and
6. the acquisition of the signature.

(2) The identification data obtained in accordance with paragraph 1 is included in the prisoner's personal files or stored in personal file systems. They are to be protected in a such to way that the knowledge is only available for the purposes referred to in paragraphs 3 and 4, as well as for the purposes of Articles 16 and 28 is possible.

(3) Data collected in accordance with paragraph 1 may only be used.
1. for the purposes for which it was collected,
2. to identify prisoners, if it is necessary for purposes of search and arrest of the escaped prisoners or prisoners who can be found outside the institution without permission or
3. for the purposes indicated in Article 10, paragraph 2, point 7 and Articles 16 and 28.

(4) Data collected according to paragraph 1 may only be transmitted to
1. law enforcement authorities, to the extent necessary for purposes of the pursuit and arrest of escaped prisoners or prisoners who can be found outside the institution without permission,
2. police authorities of the Federation and the regions to the extent necessary for the prevention of a present imminent danger to life, limb or liberty of persons in the institution or for significant property values is required,
3. public authorities referred to in Articles 16 and 28, under the conditions referred to therein, as well as
4. public authorities, at their request, in so far as the data subjects were required to tolerate or assist in the direct collection of the data to be transmitted; the requesting public body must indicate in its request the legal basis of the obligation to cooperate or to tolerate; If this obligation is based on an order issued to the persons concerned in a particular case, the requesting body shall prove at the same time that a corresponding order has been issued and is enforceable.

(5) Data collected under paragraph 1 is to be deleted immediately after the release of the prisoners; Articles 59, 60 shall remain unaffected. The erasure of data is to be documented in the prisoner's personal files.

Article 28 Data synchronization and identification

(1) If there are doubts about the identity of prisoners, the law enforcement authorities immediately transmit the data collected by them or identity data otherwise available to them within the meaning of Article 27 paragraph 1 and the data available to them within the meaning of Article 14 paragraph 3 to the State Criminal Police Office, insofar as this is necessary to establish the identity. The State Criminal Police Office compares the transmitted data with the data available there for the purposes of identification of the prisoners and reports the outcome to the law enforcement authorities.

(2) Subject to the conditions laid down in paragraph 1, sentence 1, law enforcement authorities may also request a comparison of the identification data and identity data from the Federal Criminal Police Office and the Federal Office for Migration and Refugees.

Article 29 Use of opto-electronic devices

(1) The institutions may only monitor rooms and open spaces by means of optical-electronic devices, as far as there is a legal provision allowing this for reasons of security.

(2) Each institution with opto-electronic devices creates a uniform approach to opto-electrical monitoring of structural installations. The concept must contain all operational facilities as well as the areas covered by them in a map-like format and must be continuously updated.

(3) In the planning of optical-electronic devices it is necessary to ensure that:
1. the observation takes place only insofar as this is necessary for reasons of safety, particularly in order to prevent unauthorized access to certain zones and
2. the prisoners in the institutions remain in appropriate areas where they are not monitored using opto-electronic devices.

(4) The observation of spaces and open spaces by means of opto-electrical devices shall be indicated by means of linguistic and non-linguistic signs in a way that clearly identifies the fact and the range of observation at all times.

(5) In the case of prisoner transport, the vehicles used by the prison may allow prisoners to be observed by means of opto-electronic devices; paragraph 4 and Article 32 paragraph 4 shall apply mutatis mutandis.

Article 30 Opto-electrical devices around the institution

The observation of publicly accessible space outside the boundaries of the institution by means of opto-electrical devices is only and to that extent permissible, as required by the local conditions for the exercise of the house rights or the safety of the institution, taking into account the concerns of third parties, especially to prevent escapes, exemptions and the throwing of objects to the prison premises.

Article 31 Opto-electrical devices within the institution

The observation of spaces and open areas within the institution by means of optical-electronic equipment is permitted, insofar as this is necessary for reasons of safety, in particular in order to oversee the prisoners and to prevent unauthorized access to certain zones, and Article 32 does not determine otherwise.

Article 32 Opto-electrical devices within prison cells and rooms

(1) The observation within prison cells and rooms by means of optical-electrical equipment is not permitted, unless specified otherwise below.

(2) In the context of an observation as a special security measure, the opto-electrical monitoring is permitted, to the extent it is necessary to prevent a present danger to life or limb. If the necessity ends, the opto-electrical monitoring must be stopped immediately. The opto-electrical monitoring shall be arranged and justified in writing in the framework of the arrangement of the observation; in the arrangement the scope of the observation has to be determined. It must be ended at the latest after 72 hours, unless it is extended by a new order.

(3) During the period of the opto-electrical observation, the prisoners shall be informed about it.

(4) In the design and monitoring of optical-electronic observed prison cells and rooms basically the elementary needs of the prisoners to preserve their privacy shall be taken into account, in particular, to exclude sanitation facilities from the observation; alternatively, to exclude the recognizability of these areas through technical measures. In the event of acute self-injury or suicide risk, full monitoring is permitted in the individual case. The observation of women prisoners should be done by female employees, the observation of male prisoners by male staff.

(5) The opto-electrical observation is to be interrupted, if it is, temporarily, not required in the individual case or the observation is excluded by law.

Article 33Storage of data collected via optical or acoustic devices, documentation

(1) The data collected permissibly by means of optical--electronical equipment may only be saved if this is required to archive the purposes that allowed the collection. Once that purpose is over, the data is to be deleted without delay, at the latest after 48 hours. Article 60 paragraph 1 points 1 to 3 and 5 shall remain unaffected.

(2) For the storage of the data collected permissably by means of acoustic-electronical devices, paragraph 1 shall apply mutatis mutandis. In addition, storage is also permitted, as far as and for as long as this is necessary for the transmission of the collected data to the court, which has ordered the substantive monitoring of the discussions.

(3) By way of derogation from the provisions of paragraphs 1 and 2, pursuant to Article 32 paragraph 2, the collected data will not be saved.

(4) Data collected by means of opto-electrical or acoustic-electronic equipment must not be processed further, in so far as it is subject to the core area of private life. By means of appropriate measures and tests, it must be ensured that no further processing of this data takes place. However, the stored data is to be deleted immediately. Not covered by the core area of private life are usually conversations about crimes or conversations through which crimes are committed.

(5) The processing data collected using optical-electrical or acoustic-electronic equipment is to be documented. The documentation may be used solely for the

purposes of the data protection control. It must be deleted when it is no longer necessary for these purposes, but no later than at the end of the calendar year preceding following the year of documentation.

Article 34 Reading out data storage devices

(1) electronic data storage devices as well as electronic devices with data storage devices that are in the institution without permission may, at the request of the director of the institution, be read out, as far as concrete evidence justifies the assumption that this is required for law enforcement purposes. The reasons are to be recorded in the arrangement. If the data subjects are known, they shall be informed about the reasons before reading. When reading, the legitimate interests of the data subjects, in particular the core area of private life, must be taken into account. The reading is to be limited as much as possible to the contents that are necessary to achieve the purpose which is the basis of the arrangement.

(2) The data collected pursuant to paragraph 1 may be processed for the purposes for which it was collected, insofar as this is necessary. In addition, the processing is permitted for the purposes referred to in Article 10 paragraph 2 and 3, Article 12 paragraph 3 and 6, having regard to the provisions of Article 17, insofar as this is necessary and legitimate interests of the data subjects do not hamper it.

(3) The processing of data collected in accordance with paragraph 1 is inadmissible in so far as it is subject to the core area of private life. This data shall be deleted immediately. The collection and the deletion of the data must be documented. The documentation may be used solely for the purposes of the data protection control. It must be deleted when it is no longer necessary for these purposes.

(4) Prisoners are to be informed upon arrival about the possibility of reading out unauthorized data storage devices.

Article 35Identification of non-institutional persons

(1) The entrance to the prison by non-institutional persons may be made conditional upon them indicating their:

1. first name, family name and address and they prove these, for identification, by means of official identity cards and
2. The collection of unique identification characteristics of the face, eyes, hands, voice or signature is tolerated, insofar as this is necessary or, in the case of biometric data, if this is absolutely necessary in order to prevent the escape of prisoners by leaving the institution in confusion.

(2) The processing of the identification features referred to in paragraph 1 is only permissible if it is necessary for

1. identity verification before leaving the institution or
2. Prosecution of criminal offenses for which there is a suspicion that they were committed during the stay in the institution; the data required to the prosecution of criminal offences can be transmitted to the competent law enforcement authority; this also applies to the prosecution of offenses under Article 115 of the law concerning offences.

(3) The identification features collected in accordance with paragraph 1 are to be deleted no later than 24 hours after their collection, if their transfer is not allowed by paragraph 2 point 2; in this case, they must be transferred without delay, and then they shall be deleted.

(4) Article 28 shall apply mutatis mutandis.

Article 36 Photo ID cards

(1) The institution can oblige the prisoners to carry a photo ID, if this is necessary for reasons of security or order of the institution. It shall be ensured that the ID card only contains the data necessary to achieve these purposes.

(2) The card is to be confiscated and destroyed immediately at the time of discharge or transfer to another institution.

Section 6 Protection requirements

Article 37 Earmarking

Recipients may store, use and transmit personal data only for the purpose for which they were sent. They may only store, use and transmit this data for other purposes, if the data could have been transmitted to them for that purpose as well, and in the case of a transfer to a non-public office, the law enforcement authority had approved it. The law enforcement authorities indicate the receiver on the earmarking pursuant to sentences 1 and 2.

Article 38 Safeguards

(1) Personal data in files and file system is to be protected against unauthorized access and unauthorized use. For the nature and extent of the necessary technical and organizational measures Articles 39 to 41 shall apply.

(2) Unless otherwise regulated, staff may only gain knowledge of personal data when this is necessary in order to fulfil their tasks or otherwise for the achievement of the objective of law enforcement.

(3) Health records are to be kept separately from other documents and are to be especially protected.

Article 39 List of processing activities

(1) The law enforcement authorities must keep a list of all categories of processing activities in their competence. This list shall contain the following particulars:

1. the name and contact data of the respective law enforcement authority and the name and contact data of the data protection officer of the authority,
2. the purposes of the processing,
3. a description of the categories of data subjects and the categories of personal data,
4. the categories of recipients to whom the personal data has been disclosed or is to be disclosed,

5. the categories of transfers of personal data to places in a third state or to an international organization,
6. the deadlines for the erasure or the review of the necessity of storing different categories of personal data,
7. a general description of the technical and organizational measures in accordance with Article 40,
8. the legal basis of the processing and
9. the use of profiling,

(2) The processor shall have a list of all categories of processing operations that performs on behalf of the law enforcement authorities, and it shall contain the following particulars:
1. the name and contact details of the processor and each responsible person, on whose behalf the processor works as well as data of the data protection officer,
2. Transfers of personal data to places in a third state or to an international organization with an indication of the state or the state or the organization and
3. a general description of the technical and organizational measures in accordance with Article 40.

(3) The lists referred to in paragraphs 1 and 2 shall be made in writing or in electronic format.

(4) The law enforcement agencies and processors give their lists to the state data protection officer on request.

Article 40 Data protection through technology design and privacy-friendly default settings

(1) The law enforcement authorities and the processor shall take the necessary technical and organizational measures, taking into account the state of technology, the cost of implementation, the type, scope, the circumstances and the purposes of the processing as well as the probability of occurrence and the severity of the risks associated with the processing to the legal interests of the data subjects, in order to ensure an adequate level of protection in accordance with the risk during the processing of personal data, in particular with regard to the processing of special categories of personal data.

(2) The technical and organizational measures to be taken by the law enforcement authorities ensure that:

1. only authorized personal data is known (confidentiality),
2. personal data remains intact, complete and up to date during processing (integrity),
3. personal data is available at the right time and can be processed correctly (availability),
4. personal data can be assigned to its origin at any time (authenticity),
5. it can be determined who has processed which personal data, when and in which way (audit capability),
6. the procedures with regard to the processing of personal data are complete, up-to-date and documented in a way that they can be tracked in a reasonable time (transparency),
7. personal data can not or can only be processed with disproportionately high expenditure for any purpose other than the designated purpose, unless a law or ruling allows or orders this (no connection), and
8. procedure are designed in such a way that the data subjects are permitted to exercise the rights referred to in Articles 8 and 9 (possibility of intervention).

(3) In order to implement the measures referred to in paragraph 2, the law enforcement authorities or the processor shall, in the case of automated processing, after a risk assessment, adopt measures aimed at:

1. denying unauthorized access to processing systems, with which the processing is performed (access control),
2. preventing unauthorized reading, copying, varying or deletion of data carriers (data carrier control),
3. prevention of unauthorized input of personal data as well as unauthorized knowledge gaining, modification or deletion of stored personal data (storage control),
4. the prevention of the use of automated processing systems by unauthorized persons, using data transfer equipment (user control),
5. ensuring that the party who is authorized to use an automated processing system only has access to personal data included in their access authorization (access control),
6. ensuring that it is possible to check and determine to which places personal data has been transmitted or made available or can be transmitted and made available by means of data transmission equipment (transmission control),

7. ensuring that it can be subsequently checked and determined which personal data has been entered or changed in automated processing systems, and when and by whom (input control),
8. ensuring that the transfer of personal data as well as the transport of data carriers the confidentiality and integrity of data is protected (transport control),
9. ensuring that used systems can be restored in the event of a fault (recoverability),
10. ensuring that all functions of the system are available and the appearance of faults in the functions is reported (reliability),
11. ensuring that personal data stored cannot be damaged by the malfunctioning of the system (data integrity),
12. ensuring that personal data that will be processed as part of the order will only be processed according to the instructions provided by the customer (order control),
13. ensuring that personal data is protected against destruction or loss (availability control), and
14. ensuring that personal data collected for different purposes can be processed separately (severability).

A purpose referred to in sentence 1, points 2 to 5 can be achieved in particular through the use of encryption methods corresponding to the status of technology.

(4) The law enforcement authorities shall take appropriate technical and organizational measures to ensure that only such personal data may be processed through default settings, in principle, the processing of which is necessary for the specific processing purpose. This affects the amount of collected data, the extent of its processing, its storage period and its accessibility. The measures must particularly ensure that the data cannot be made accessible automatically to an indefinite number of persons through the default settings.

(5) The technical and organizational measures are to be determined based on a security concept to be documented, in which the components are provided with the estimation of probability of occurrence and the severity of the risks associated with the processing to the right of informational self-determination. The effectiveness of the measures shall be checked taking into account the changing framework conditions and developments in the technology. The resulting necessary adaptations shall be implemented promptly, insofar as this is possible with a reasonable effort. Article 41 remains unaffected.

Article 41 Privacy-impact assessment with high risk

(1) If a form of processing, in particular in the case of use of new technologies, due to the nature, scope, the circumstances and the purposes of the processing is likely to have a significant risk for the legal interests of data subjects, the law enforcement authorities perform an assessment of the impact of the intended processing operations beforehand for the data subjects.

(2) For several similar processing operations with similar high-risk potential, a common data protection impact assessment can be carried out.

(3) The law enforcement agencies involve the data protection officers of the authority in the implementation of the data protection impact assessment.

(4) The data impact assessment shall consider the rights of the people affected by the processing, and must contain at least the following:

1. a systematic description of the planned processing operations and the purposes of the processing,
2. an assessment of the necessity and proportionality of the processing operations in terms of their purpose,
3. an assessment of the risks to the legal interests of the data subjects and
4. the measures with which risks are to be avoided, including the warranties, security measures and procedures through which the protection of personal data shall be ensured, and the compliance with the legal requirements shall be demonstrated.

Article 42 Logging

(1) In automated processing systems, the following processing operations are to be logged:

1. collection and storage,
2. change,
3. query,
4. disclosure including transmission,
5. combination and
6. deletion or restriction of processing.

(2) The logs of queries and disclosures must make it possible to determine the date and time of these processes and, as far as possible, the identity of the person who requested or disclosed the personal data, and the identity of the recipient of the data. From the identity of the person, the justification for a query or disclosure shall also be derivable.

(3) The logs may only be used by the data protection officers of the authority or of the country for the review of the lawfulness of the processing, as well as for the self-monitoring and for ensuring the integrity and security of personal data. The log data may also be used for the prosecution of criminal offenses or for official legal or disciplinary measures in connection with a breach of data confidentiality and for the prosecution of illegal acts that are of considerable importance.

(4) The log data shall be deleted two years after creation.

(5) The logs are to be made available to the state data protection officer on request.

Article 43 Identification within the institution

(1) Personal data of prisoners may only be made available within the institution, insofar as this is necessary for the orderly cohabitation in the institution and is not in contrast with the provisions of this law.

(2) Special categories of personal data of prisoners may not be made generally available in the institution.

Article 44 Findings from overseeing, monitoring and control measures

(1) Personal data that became known from the supervision or monitoring of visits, the monitoring of telecommunication, the visual inspection or monitoring of written correspondence or checking the contents of packages in a permissible way shall be clearly marked as such in files and file systems of enforcement, as well as in the case of a transmission. This data may only be processed
1. with the consent of the prisoners,
2. for measures of enforcement and integration planning,
3. to maintain the security or public order of the institution or

4. for the purposes indicated in Article 10 paragraph 2, points 2 to 7 and Article 16.

(2) Data that became known in a permissable way in accordance with paragraph 1, sentence 1, may also be processed in the enforcement of pre-trial detention and deprivation of freedom in accordance with Article 1, paragraph 1, point 2, in addition to the purpose specified in paragraph 1, sentence 2 for purposes of
1. averting risks to the role of the implementation of pre-trial detention or
2. Implementation of an arrangement in accordance with Article 119 of the Code of Criminal Procedure.

(3) If the data referred to in paragraph 1 belongs to the core area of private life, it may not be recorded, logged or otherwise stored and it may not be processed in another way. Not covered by the core area of private life are usually conversations about crimes or conversations through which crimes are committed. Contrary to sentence 1, stored data shall be deleted immediately. The facts of the acquisition and the deletion of the data must be documented. The documentation may be used solely for the purposes of the data protection control. It must be deleted when it is no longer necessary for these purposes.

Section 7 Special provisions for secret bearers

Article 45 Secret bearers

(1) Those people who are engaged—in within the law enforcement or outside of law enforcement— in the examination, treatment or counselling of prisoners, namely
1. physicians, dentists, pharmacists or other health professionals who need state-regulated training in order to practice their profession or to hold a professional title;
2. certified psychologists,
3. State-recognized social workers or state-recognized social pedagogues as well as
4. pastors

are subject to secrecy regarding the secrets entrusted to them by prisoners or otherwise known about prisoners, among themselves and towards the institution and the supervisory authority, unless otherwise specified. This applies accordingly to their professional assistants and the persons who work for them in preparation for the profession, but not towards those holding professional secrets.

(2), The institution draws attention of external secret bearers according to paragraph 1 sentence 1 numbers 1 to 3 (those holding secrets) to the disclosure obligations and powers.

Article 46 Disclosure obligation

(1) Persons holding professional secrets have to disclose personal data known to them on their own or on request to the leader of the institution, even if they have been entrusted with it within the framework of the professional relationship of trust or have become otherwise known, as far as this necessary, also taking into account the interests of the prisoners at the secrecy of personal data, to prevent
1. a danger to the life of a person, especially for the prevention of suicides,
2. a significant danger to body or health of a person or
3. the danger of committing criminal offences that are of considerable importance.

(2) State-recognized social workers, as well as state-recognized social pedagogues working as law enforcement staff, must disclose personal data known to them on their own initiative or on request to the leader of the institution, to the extent that this is necessary for law enforcement purposes. If they work in the context of special treatment offers, paragraph 1 applies.

(3) Those holding professional secrets outside the law enforcement system may also fulfil the obligation under paragraph 1 towards those who hold professional secrets and are employed in the institution.

Article 47 Authority to disclose

(1) The professional secret holders are authorized to disclose personal data entrusted to them or otherwise known to them within the framework of the professional relationship of trust to the head of the institution, insofar as
1. the prisoners' consent or
2. this is absolutely necessary for law enforcement purposes and the interests of the prisoners in secrecy do not prevail.

(2) If professional secret holders treat the same prisoners at the same time or in succession, they are not subject to secrecy in relation to each other and are entitled

to comprehensive mutual information, provided that the prisoners have given effective consent, this is necessary for the purpose of a targeted joint treatment and if they are not entrusted with other tasks in the law enforcement system in relation to the prisoners concerned.

Article 48 Notification for prisoners regarding disclosures

(1) Prior to the collection of personal data, prisoners shall be informed by the professional secret holders in writing about the disclosure duties and powers under this law. If professional secret holders from outside the institution are involved, the notification pursuant to sentence 1 shall be done by the institution.

(2) The prisoners are to be notified about a disclosure in accordance with Article 46 paragraph 1 point 2 and paragraph 3 and Article 47. It is not required to provide notification if the prisoners gained knowledge of the disclosure in another way. The notification may be omitted, as long as the purpose of the measure was thwarted. The notification is to be made up for immediately, as soon as the purpose of the measure is no longer applicable.

Article 49 Earmarking of disclosed personal data, approval of disclosure recipients

(1) Personal data disclosed pursuant to Articles 46 and 47 may only be used for the purpose for which they were disclosed or for which the disclosure would have been permitted, and the data may only be stored, used and transmitted under the same conditions, under which professional secret holders themselves were authorized for this.

(2) The leader of the institution can generally permit, under these conditions, the immediate disclosure to certain employees.

Article 50 Access to data in case of emergency

(1) All persons working in law enforcement may receive information also about special categories of personal data for the purpose of transmitting these data directly and without delay to the emergency rescue personnel, as far as the prisoners

1. agree to this or
2. are unable to give informed consent and knowledge provision is absolutely necessary to prevent a present danger to the life of a human being or a present significant risk to the health of a human being.

(2) If it is necessary to ward off a present danger to life or a present significant threat to the health of a human being, prison personnel may obtain knowledge of personal data collected by professional secret holders.

(3) The further processing of the data obtained in this way is not permitted. The note is to be included in the prisoner's personal files.

Section 8 Rights of the data subjects

Article 51 General information on data processing

The responsible law enforcement authorities make available to prisoners and other affected persons in general and comprehensible form information about

1. the purposes for which the personal data is processed,
2. The rights of the data subjects to information, rectification, cancellation and limitation of processing,
3. their name and contact data and the contact data of the data protection officer of the authority,
4. The right to phone the data protection officer, and their contact data.

Article 52 Obligation to inform in data collection with knowledge of the data subjects

If personal data will be collected from data subjects with their knowledge, they shall be informed in an appropriate manner about the purpose of the data collection and the existence of the right to information and rectification. If the personal data is

collected by virtue of provisions laid down by law that legally obliges to provide information, or the granting of information is a prerequisite for the granting of legal benefits, then the data subjects shall be informed about this, and otherwise about the voluntariness of their information. If the information must be given for the granting of a performance, the data subjects shall be informed about the possible consequences of a failure to reply.

Article 53 Notification at data processing without the knowledge of the data subjects

(1) The prisoners and other data subjects are informed about the collection of personal data without their knowledge or the transmission of data for purposes for which it has not been collected, under the specification of this data. This notification shall include, in addition to the general information listed in Article 51 particularly the following information:

1. the legal basis of the processing,
2. the data storage duration or, if this is not possible, the criteria for determining this duration and
3. the recipient of the personal data.

(2) In the cases referred to in paragraph 1, the law enforcement authorities may postpone or restrict the notification, or refrain from doing so, as far and as long as otherwise

1. the achievement of the enforcement purposes referred to in Article 2 point 2 would be endangered,
2. procedure for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or offenses or the enforcement of criminal sanctions would be endangered,
3. public security would be endangered,
4. it would be disadvantageous to the interest of the Federal Republic or of a region or
5. The rights of any other person would be endangered or impaired,

and the interest in avoiding these dangers and disadvantages outweighs the interests of the data subjects in the notification.

(3) If the notification relates to the transfer of personal data to authorities of the Public Prosecutor's Office, police authorities, state financial authorities, as far as they store

personal data in fulfilment of their statutory duties within the scope of the Tax Code for monitoring and testing, constitutional protection authorities of the Federation and the regions, the Federal Intelligence Service, the Military Shielding Service and, as far as the security of the Federation is concerned, other authorities of the Federal Ministry of Defence, it is permissible only with approval of these bodies. This applies to the collection of personal data by the authorities referred to in sentence 1 and shall apply mutatis mutandis.

(4) In the case of the limited notification referred to in paragraph 2, this shall be governed by Article 54 paragraph 6 accordingly. The law enforcement authorities document the reasons for the decision referred to in paragraph 2.

Article 54 The data subjects' right to information

(1) The law enforcement authorities shall issue notification, at the request of the data subjects, to ascertain whether they process personal data about these persons. In the case of a data processing according to sentence 1, data subjects also have the right to obtain information about

1. the personal data, the subject-matter of processing operations, and the category to which they belong,
2. the information available about the origin of the data,
3. the purposes of the processing and the legal basis thereof,
4. the recipients or categories of recipients to whom the data was disclosed,
5. the data storage duration or, if this is not possible, the criteria for determining this duration,
6. the right to rectification, deletion or restriction of the processing of the data by the law enforcement authorities,
7. The right to phone the state data protection officer, as well as
8. details of the contact data of the state data protection officer.

(2) Paragraph 1 does not apply to personal data processed only because they may not be deleted on the basis of statutory retention requirements, or that solely serve data backup or data protection control purposes, if the provision of information would require a disproportionate effort and the processing for other purposes is excluded through appropriate technical and organizational measures.

(3) The provision of information is to be omitted if the data subjects do not provide any information to enable the locating of the data, and therefore the burden of providing the information is disproportionate to the interest of the data subjects in the information.

(4) The law enforcement authorities may, under the conditions set out in Article 53 paragraph 2 and 3 omit, postpone or restrict this notification.

(5) The law enforcement authorities shall inform the data subjects in writing without delay of the omitting or limitation of information. This does not apply if the granting of this information is a risk, a disadvantage or an impairment within the meaning of Article 53 paragraph 2. The information referred to in sentence 1 shall be justified, unless the statement of reasons would jeopardize the purpose of omitting or limitation.

(6) If the data subjects referred to in paragraph 5 are informed about the disregard of or limitation of information, they can also exercise the right to information through the state data protection officer. The law enforcement authorities shall inform the data subjects about this possibility as well as about the fact that they can phone the state data protection officer or seek legal protection. If the data subjects, according to sentence 1, use their right, this must be told to the state data protection officer. The data protection officer shall inform the data subjects that all necessary tests are done, or a review has taken place by them. This release may contain the information that data protection law infringements have been recorded but may not draw conclusions about the state of knowledge of the law enforcement authorities, insofar as they do not allow any further information. The law enforcement authorities may refuse consent only to the extent and for the duration as they can omit or restrict notification according to in paragraph 4. The state data protection officer shall also inform the data subjects of their right to judicial protection.

(7) The information can also be given by granting access to the file or by handing over copies or printouts. In doing so, the interests of the prisoners and other data subjects in a particular form of information must be taken into account.

(8) The law enforcement documents the reasons for the decision.

Article 55 File inspection rights

(1) If information shall be granted to the data subjects in accordance with Article 54, upon request, they will be granted access to the file if the awareness is insufficient to fulfil their legal interests, the inspection is absolutely necessary and does not conflict with prevailing legitimate interests of third parties. As far as file components have a lock mark, they are not subject to the file inspection.

(2) Interested persons may, at their own expense, consult during the file inspection
1. a person from the group of
   a) the lawyers
   b) the notaries,
   c) the selected defenders (Article 138 paragraph 1 and 2 of the Code of Criminal Procedure),
   d) legal advisers allowed by judicial decision under Article 149 paragraph 1 or 3 of the Code of Criminal Procedure or
   e) legal advisers in accordance with Article 69 of the Youth Court Law,
2. Primary carers as well as
3. an interpreter under general oath.

The data subjects concerned may also let their right to file inspection be exercised by a person from the group of persons referred to in sentence 1, numbers 1 and 2 alone (file inspection right by agents). Consulting or commissioning other prisoners is prohibited, even if they belong to the group of persons mentioned in sentence 1.

(3) In the event of file inspection, the data subjects have the right to make notes from the files.

(4) The data subjects may receive copies or prints of individual documents from the files or file systems about them, at the written request, if there is a legitimate interest. Such an interest is to be assumed, if the data subjects are dependent on photocopies or prints for the assertion of rights vis-à-vis courts and authorities.

(5) File inspection is free of charge. The production of copies and prints is available for a fee. The data subjects pay the expected costs in advance. If the prisoners are not able to do so, the law enforcement authorities can, in justified cases, cover the costs to a reasonable extent.

Article 56 Information and file inspection in health records

The prisoners receive upon request information about their or access to their health records. For the right to file inspection Article 55, paragraph 1, sentence 2, paragraphs 2, 3 and 5 shall apply mutatis mutandis.

Article 57 Lock marks

(1) Lock marks may only be affixed, in so far as this is
1. for medical reasons alone for the good of the prisoners,
2. for the protection of interests worthy of protection, as well as for the protection of body or life of third parties or
3. based on provisions laid down by law, that give the obligation to maintain secrecy,

and it is absolutely necessary, also taking into account the interests of the data subjects in the information. The lock mark in accordance with sentence 1 point 1 shall be affixed by the professional secrecy holders who have added the file parts to be blocked to the file; the other lock marks are affixed by the prison director.

(2) The basis and extent of the locking are to be noted in the file. This note is in the lock. Locked parts of the file must be stored separately from the other files, provided that the files are kept in paper form; otherwise, they are to be secured particularly.

Article 58 Procedures for the exercise of the rights of the data subjects

(1) The law enforcement authorities communicate with the data subjects in a precise, understandable and easily accessible form using clear and simple language. Without prejudice to specific formal requirements, they should use the form chosen for the application when responding to applications.

(2) The law enforcement authorities shall inform the data subjects promptly in writing about what happened with the application. Articles 54 paragraph 5 and Article 62 paragraph 3 shall remain unaffected.

(3) The granting of general information in accordance with Article 51, the obligation to provide information in the case of data collection in accordance with Article 52, the notifications pursuant to Articles 53 and 64, paragraph 1, sentence 2, point 1, second part and the processing of applications pursuant to Articles 54 and 62 are free of

charges. For manifestly unfounded or excessive applications pursuant to Articles 54, 55 and 62, the law enforcement authorities may refuse to act based on the application. In this case, the law enforcement authorities shall be able to prove the manifestly unfounded or excessive character of the application.

(4) If the law enforcement authorities have reasonable doubts as to the identity of the person concerned who made a request pursuant to Articles 54 or 62, they can request additional information from that person which is required to confirm their identity.

Section 9 Deletion, limitation of processing and rectification

Article 59 Deletion

(1) Personal data shall be deleted, as far as its further processing is no longer permissible, or for any reason it is not required

1. for the fulfilment of law enforcement purposes or
2. for the implementation of scientific research in accordance with Article 22 or statistical purposes

.

(2) The necessity of the deletion is to be monitored annually. The deadline for the control of personal data pursuant to sentence 1 begins with the dismissal or relocation of the prisoners in another institution, in other cases with the collection of personal data.

(3) Personal data shall be deleted no later than five years after the dismissal or the relocation of the prisoners; in the execution of a juvenile sentence, the period is three years and at juvenile detention, it is two years. Until the expiry of the retention period of the prisoner's personal file, the family name, first name, birth name, date of birth, place of birth, entry and exit date of the prisoners may be an exception, insofar as this is necessary for finding the prisoner's personal file.

(4) The personal data shall be deleted immediately, if, in the enforcement of pre-trial detention and deprivation of the freedom in accordance with Article 1, paragraph 1, point 2, the law enforcement authorities become aware of a not only provisional closure of the procedure, an indisputable rejection of the opening of the main

proceedings or a legal acquittal. In addition, in these cases, at the request of the prisoners, the authorities who have received a notification pursuant to Article 20, shall be informed about the procedure output. Prisoners are to be informed of their right to make an application during the hearing or a subsequent notification (Article 20 paragraph 6).

Article 60 Limitation of processing

(1) Instead of deleting the stored personal data, its processing shall be restricted, if necessary,

1. because there are actual clues to risk prevention, security, to the prevention and prosecution of criminal offenses or to the achievement of the purposes referred to in Article 10, paragraph 2, point 4,
2. to determine, enforce or defend legal claims in connection with the law enforcement,
3. because there is reason to believe that the deletion would affect the legitimate interests of data subjects,
4. for the purposes of data backup or data protection control,
5. for other evidence purposes,
6. because a deletion is not possible or only with disproportionately high expenditure, due to the special type of storage or
7. because the deletion in accordance with Article 59 is opposed to the retention period of a different legal standard.

The purpose of the restriction of the processing is to be documented.

(2) In the processing referred to in paragraph 1, limited data may be processed only for the purpose which stood in the way of its deletion; it may also be processed to the extent necessary to remedy a lack of evidence for prosecution of criminal offenses or if the data subjects agree. In case of automated file systems, it is to be technically ensured that the restriction of processing is clearly recognizable and the processing for other purposes is not possible without further examination. The purpose of the processing is to be documented, as well as in the case of transmission to the recipient.

(3) The processing of personal data by way of derogation from paragraph 2 is possible unrestrictedly, and the restriction of the processing should be terminated if

1. the data subjects have given their consent or

2. the prisoners are re-admitted to the prison.

(4) Data restricted 1 in the processing according to paragraph must not be kept for over ten years. This does not apply if there are concrete indications that the storage is still necessary for the purposes mentioned in paragraph 1. The retention period begins with the calendar year following the year of the expiration. The provisions of the State Archives Act shall remain unaffected.

Article 61 Rectification

(1) Personal data shall be corrected if it is incorrect, incomplete or not up to date. In statements or assessments this relates to the question of the accuracy, not the contents of the statement or assessment. As far as this is possible with reasonable time and effort, the personal data is to be checked before processing for correctness, completeness and up-to-datedness. In files, it is sufficient to indicate in an appropriate manner, at what point in time or for whatever reason the data were incorrect or have become incorrect. A completion of personal data can also be carried out by means of a supplementary declaration.

(2) If the accuracy or inaccuracy of personal data cannot be determined, the restriction of processing shall take the place of the correction. Before the abolition of the restriction, data subjects are to be informed.

Article 62 Rights of the data subjects to rectification and deletion as well as limitation of processing

(1) The data subjects have the right to demand that the law enforcement authorities correct without delay inaccurate data relating to them in accordance with Article 61. The data subjects may also require the completion of incomplete personal data, if this is appropriate, taking into account the processing purposes.

(2) The data subjects may, under the conditions laid down in Article 59, request the deletion of the data.

(3) The law enforcement authorities shall inform the data subjects in writing of omitting the rectification or deletion of personal data or to the restriction of processing

taking its place. This does not apply if the granting of this information involves a risk within the meaning of Article 53 paragraph 2. The information according to sentence 1 shall be justified, unless the statement of reasons would endanger the purpose of omitting notification. Articles 54 paragraph 6 and 8 shall apply mutatis mutandis.

Article 63 Notifications

(1) The law enforcement authorities shall give information about the rectification of personal data to the body who previously transmitted the data to them. The same applies in the cases of deletion or restriction of the processing due to invalid processing or the rectification of the data for the recipients of data. The recipient shall delete the data under its own responsibility, limit its processing or correct it.

(2) The compliance with the stipulations is to be ensured through appropriate technical and organizational steps.

Section 10 Application of further provisions and final provisions

Article 64 Application of other provisions of the general data protection law

(1) Unless otherwise provided in this law, the general data protection regulation shall apply. In particular, the following provisions for

1. the reporting of violations of the protection of personal data to the supervisory authority (Article 65 of the German Federal Data Protection Act of June 30, 2017 [BGBl. P. 2097]) and notification of the persons affected by a breach of personal data protection (Article 66 of the German Federal Data Protection Act),
2. the appointment, order and the tasks of the data protection officer of the authority (Articles 5 to 7 of the German Federal Data Protection Act),
3. the transmission of personal data to bodies in third countries or to international organizations (Articles 78 to 81 of the German Federal Data Protection Act),
4. the data protection legal supervision of law enforcement authorities by the state data protection officer (Articles 8 to 16 of the German Federal Data Protection Act),
5. cooperation with the state data protection officer (Articles 68 and 69 of the German Federal Data Protection Act),

6. the claim for damages, compensation, and the criminal law provisions (Articles 83 and 84 of the German Federal Data Protection Act),
7. the invocation of the state data protection officer and for the legal protection against their decisions (Articles 60 and 61 of the German Federal Data Protection Act)

find appropriate application.

(2) For the processing of personal data by law enforcement in the material scope of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Council Directive 95/46/EC (Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1; L 134, 22.11.2016, p. 72; L 127, 23.5.2018, p. 2) its provisions shall solely be governing and the provisions adopted for this purpose.

Article 65 Entry into force, expiry

(1) Subject to the provisions of paragraph 2 of this law, it shall enter into force on the … /day after the promulgation. At the same time, regional laws become invalid.

(2) Article 42 shall enter into force on May 6, 2023.

Justification

A. Introduction

The European Parliament and the Council of the European Union issued two regulations on 27 April 2016 for protection regarding the processing of personal data:

On the one hand, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Council Directive 95/46/EC (OJ L 119, 4. May 2016, p. 1; L 314, 22.11.2016, p. 72; L 127, 23. 5. 2018, p. 2) (General Data Protection Regulation (GDPR)) and, on the other hand, the directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal sanctions as well as on the free movement of such data and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4. May 2016, p. 89;
L 127, 23.5.2018, p. 9) (Directive (EU) 2016/680).

The present template design is used for the implementation of EU Directive (2016/680).

Directive (EU) 2016/680 also applies to criminal, juvenile, remand enforcement, preventive detention and juvenile detention (prisons); law enforcement is part of the execution of the sentence or at least falls under the protection and defence against threats to public safety. Essentially the following arguments are in favour of this evaluation:

The classification of law enforcement under the concept of criminal enforcement is not foreign to the German legal system. Thus, in the commentary literature on Articles 449 et seq. of the Code of Criminal Procedure, a distinction is mainly made between the execution of sentences in the broad sense and the execution of sentences in the narrow sense (see Meyer-Goßner / Schmitt, 60th edition 2017, StPO, before Article 449 recital

2). The concept of execution of sentences in the broader sense is synonymous with the concept of realization of a sentence and also includes, in addition to the execution of sentences in the narrower sense the prison (see Appl, in: Karlsruhe Commentary on the Code of Criminal Procedure, 7th Edition 2013, before Art. 449 recital 3; Pollähne, in: Gercke/Julius/Temming, among others, Code of Criminal Procedure, 5th edition 2012, before Article 449 recital 1).

A European legal consideration also leads to a classification of the judicial enforcement under the concept of enforcement within the meaning of Directive 2016/680 (EU). It also supports that in numerous European countries a conceptual distinction is not performed and both matters are regulated in uniform laws. In addition, a meaning- and purpose-oriented consideration leads to this evaluation: The sensitive area of criminal justice should fall under Directive 2016/680 (EU)—and not Regulation (EU) 2016/679 that is valid since May 25, 2018—in order to give the Member States more room for manoeuvre. It is therefore obvious that this also applies for the prisons, that are the last section of criminal proceedings or measures to secure implementation of criminal proceedings and are a part of the criminal justice system.

These considerations also apply to the implementation of preventive detention and youth detention, although they do not implement penalties in the strict sense, but they are measures considered to be a state response to violations of criminal law provisions. The remand prison and their equivalent types are linked to the urgent suspicion of a breach of criminal law provisions and serve the proper implementation of criminal proceedings or the prevention of threats to public safety and order. Overall, it is open for the area of the judicial execution of the scope of the Directive 2016/680 (EU).

To the extent that the scope of Directive 2016/680 (EU) is opened, it usually excludes the validity Regulation (EU) 2016/679, which entered into force on 25. May 2018. However, it follows from Article 9, paragraph 1, sentence 2 and paragraph 2 of the Directive 2016/680 (EU), that even if there is a fundamental opening of its scope, in some cases, Regulation 2016/679 (EU) applies in connection with the respective national legal data protection provisions. If, for example, personal data originally created for one of the purposes of Directive 2016/680 (EU) was collected and processed for other purposes, Regulation (EU) 2016/679 (recital 34 of Directive (EU) 2016/680) applies.

Unlike Directive (EU) 2016/680, Regulation (EU) 2016/679 shall be binding in its entirety and directly applicable in all Member States; in accordance with Article 288 of the Treaty on the functioning of the European Union (TFEU) no transposition into Member State law is required. The aim of Regulation (EU) 2016/679 is a uniform and high level of data protection for natural persons and the removal of barriers to the movement of personal data within the European Union as a whole (recital 10 and 13 of Regulation (EU) 2016/679). Nevertheless, Regulation (EU) 2016/679 includes opening clauses for the national legislature with control options and specific control orders, so that the general and sector-specific data protection law can be adapted as far as necessary. This resultant adjustment requirement can be found in the respective national laws, notably the State data protection laws, but also in special State or Federal statutory trade laws, the legal basis for the data processing; these legal bases are then always in connection with the directly applicable Regulation (EU) 2016/679 for the processing of personal data for purposes other than those laid down in Directive 2016/680 (EU) should be used.

The scope of the Regulation (EU) 2016/679, is in accordance with Article 9(2) of Directive (EU) 2016/680 somewhat open if the data processing from the outset is not within the scope of Article 1 paragraph 1 of Directive 2016/680 (EU) governed by the administration of staff data, because they are employees of the prison. In addition, Regulation (EU) 2016/679 can apply in conjunction with sector-specific national data protection rules because personal data that is collected for the purposes of law enforcement and processed for purposes other than those of Directive (EU) 2016/680, for example in the transmission of personal social services to the competent authorities in accordance with Article 12 paragraph 3 point 2 (d) or the foreigners authority for asylum or immigration legal measures in accordance with Article 12, paragraph 3, point 2 (g).

As a result of Directive 2016/680 (EU), the area of the law enforcement and the normalized area-specific data protection provisions of a corresponding target binding implementation is required. Each Directive pursuant to Article 288 of the TFEU is also the Directive 2016/680 (EU) for each Member State to which it is addressed as to the result to be achieved. However, the legal form of the Directive leaves it to the national authorities to choose the form and methods for the implementation in national law.

The Federal government continues to have legislative competence for data protection in the enforcement of the planning, backup, and enforcement detention

(civil detention). Therefore Regulation (EU) 2016/679 applies to civilian prisoners' conjunction with the customized provisions of the penal law of the State.

B. Solution

The national implementation in the sector-specific law of data protection in the prison system provides for the present draft model for a law enforcement data protection law. The template model intends to ensure that the data protection law applicable to the law enforcement is largely complete.

With the submitted draft, the previous data protection standards are transferred into a new independent law enforcement data protection law and at the same time the provisions of the Directive (EU) 2016/680 are transposed into State law. As a result, the high value of the data protection in law enforcement is taken into account and the standalone act makes the complex matter of data protection easy-to-use.

At its 125th session in Potsdam from May 10 to 12, 2017, the Federal Prison Committee decided to set up a transnational working group to draft a model bill for the implementation of Directive (EU) 2016/680 for the prison system in Brandenburg, Berlin, North Rhine-Westphalia and Schleswig-Holstein.

In addition to the results of the working group, the draft template also considers the drafts of the regions on sector-specific data protection in prisons, which have already progressed during the preparation phase.

In the preparation of the template, the provisions of the new Federal Data Protection law of June 30, 2017 (BGBl. I p. 2097) were also considered.

This template design is the basis for further legislative work in the regions regarding the implementation of the Directive (EU) 2016/680; any local peculiarities of already existing guideline-compliant data protection regulations and classifications remain unaffected.

As a template for said template design, the Prison Law for Data Protection Schleswig-Holstein of July 21, 2016 was used (GVOBl. P. 618, 644) as the most recent stand-alone data protection act. Existing already guideline-compliant rules along with a few linguistic changes have not required new regulations with regard to

the implementation of the Directive (EU) 2016/680 (for example, the special provisions for secrecy).

The template draft contains provisions relating to general principles of data processing, the legal bases of individual processing forms (collection, storage, use and transmission), special forms of data processing (for example, data processing in the order), the requirements for data processing as further duties of law enforcement (for example, earmarking or directory of processing activities) and the rights of the data subjects enhanced with the directive implementation.

In order to maintain the existing high level of data protection law and to maximize its user-friendliness, the draft, while relying on the new central notion of processing of Directive (EU) 2016/680, still sets out the conceptual distinction between collection, storage, use and transmission. As a result, the data processing in its individual steps with the prerequisites attached thereto is still traceable in the law, i.e. first, the data is collected, then it is stored and used, then possibly transmitted and deleted after release of the prisoners.

Directive (EU) 2016/680 requires guarantees with which the data protection principles about protecting the rights of prisoners can be implemented. The draft therefore provides an implementation of—depending on the previous legal situation— the standard data protection model, which is supplemented by further technical safety standards.

Provisions are added to the comparison of data with the safety authorities, regardless of the required implementation of Directive (EU) 2016/680. These regulations (safety-relevant findings, examination of prisoners, review of non-institutional persons, case conferences, further admissibility requirements for data processing with the security authorities and the identification data reconciliation (Articles 13-17, 28)) also refer to a resolution of the Penal Equality Committee at the Spring Conference in 2017.

C. To the individual provisions

Section 1
General provisions

On Article 1 **Scope**

The provision regulates the application of the law and defines essential law enforcement terms. It takes up Article 1 paragraph 1 and 2 JVollzDSG SH in the previous version.

The scope of application of the law referred to in paragraph 1 includes the processing of personal data in all regions covered by the legislative competence of law enforcement. This law regulates the whole of the matter of data protection for law enforcement in implementation of the Directive (EU) 2016/680, which is area-specific, final and uniform. Article 64 provides for the application of the other provisions of the general data protection law. Number 1 names the traditional types of detention and accommodation in prisons, and number 2 gives a list of the types of detention that correspond to the execution of pre-trial detention. This law is not applicable to civil detention because of the lack of legislative powers of the regions in this matter. For this detention according to Article 171 StVollzG, the data protection regulations of the Federal Penitentiary Law supplemented by the provisions of the Federal Data Protection Act and the Regulation (EU) 2016/679 apply.

Paragraph 2 defines the term of law enforcement authorities used in paragraph 1 and, for reasons of better readability of the legislative text, the shorter terms "institutions" and "supervisory authority". The Ministry responsible for the law enforcement is—according to the terminology of the Penal Laws of the regions—and thus deviating from the definition of Article 3 point 15 of Directive (EU) 2016/680 -is here "supervisory authority".

On Article 2 **Definitions**

The provision defines key procedural and data protection terms in order to facilitate the readability of the law and the uniform handling of the provisions. Some definitions are used for the implementation of Article 3 of Directive (EU) 2016/680. In points 3, 5 to 7, 9 to 13 and 15 to 18, the definitions of Directive 2016/680 (EU) are taken over unchanged.

Number 1 defines the term "prisoners" as all persons that are subjects to the enforcement of the law enforcement types in Article 1 paragraph 1. These individuals are grouped together under the term "prisoners", because a large number of regulations applies to them in the same way.

Number 2 defines the enforcement purposes and thus defines the scope and limits of data processing for enforcement purposes. This implements Article 8 of the i Directive (EU) 2016/680, according to which the purpose of data processing, among other things, shall be included in legal regulations.t. If the data processing is carried out for the stated purposes, it is always governed by the scope of this law (see recital 29 of Directive (EU) 2016/680).

Number 2a describes the definitive purpose of rehabilitation, i.e. the ability of prisoners to lead a life of social responsibility without crime in the future. This enforcement purpose is anchored in both international and European law (see Rule Number 88 of the UN Standard Minimum Rules for the treatment of prisoners, "Nelson Mandela rules" and number 102.1 of the European Prison Rules of constitutional law) as well as constitutionally offered at national level. This includes health care, employment and all other aspects directly related to detention.

Number 2b defines the protection of the general public against further criminal offenses of the prisoners as a further enforcement purpose. This refers directly to the period of detention, as well as to the period after dismissal. Number 2a and 2b are to be viewed in context. There is no contrast between the integration target of enforcement and the aim of the general awareness to protect against further criminal offenses. Successful rehabilitation also ensures the comprehensive protection of the general public. Both ultimately serve the safety of the population. The State fulfils its duty of protection, in particular by promoting rehabilitation.

Number 2c defines the protection of the body, life, liberty, and property of employees and prisoners, as well as the property of the regions, by maintaining safety and order within the institution as an enforcement purpose. At the same time, the protection of individual rights serves to maintain security and order in enforcement and is consistent with the goal of rehabilitation.

Number 2d defines the prevention of the liberation and escape of prisoners as an enforcement purpose. This is the assurance of enforcement.

Number 2e defines the avoidance of non-return and misuse of easing as an enforcement purpose. The enforcement purpose serves the assurance of enforcement and the protection of the general public.

Number 2f defines the participation of law enforcement in other tasks entrusted to it by law as an enforcement purpose.

The second clause after point 2f indicates that the law enforcement purpose of pre-trial detention lies in ensuring the criminal proceedings.

Number 3 defines that the notion of "personal data" shall mean any information relating to an identified or identifiable natural person (see recital 21 of Directive (EU) 2016/680) and, for reasons of readability, introduces the term "data subject".

Number 4 defines the notion of "processing" with or without the help of automated procedures and identifies case studies (see recital 34 of Directive (EU) 2016/680). Number 4a and 4b designate the various operations within the notion of data processing.

Number 5 defines the notion of "limitation of processing". It corresponds to the previous concept of "closure".

Number 6 defines the notion of "profiling".

Number 7 defines the notion of "pseudonymization".

Number 8 defines the notion of "anonymization". The definition was derived "a.F." from Article 3 paragraph 6 of the German Federal Data Protection Act. The

principles of data protection do not apply to anonymous information (see recital 21 of Directive (EU) 2016/680).

Number 9 defines the notion of "file systems". The term is technology neutral and should apply equally for automated and manual processing (see Recital 18 of Directive (EU) 2016/680). The term corresponds to the previous definition of the term "File" referred to in Article 2(c) of Directive 95/46/EC and in data protection law applicable so far.

Number 10 defines the notion of "responsible person" for the scope of this law. For the protection of the rights and freedoms of data subjects, Directive (EU) 2016/680 sets out a clear competence of the responsibility for the data processing (see recital 54 of Directive 2016/680 (EU).

Number 11 defines the notion of "processor" as a data processor on behalf of the responsible person.

Number 12 defines the notion of "recipient".

Number 13 defines the notion of "violation of the protection of personal data".

Number 14 defines the concept inherited from Article 10 of Directive (EU) 2016/680, t of "special categories of personal data". This data is particularly sensitive because of its content.

Number 15 defines the notion of "genetic information". These are among the special categories of personal data referred to in paragraph 14.

Number 16 defines the notion of "biometric data". These are among the special categories of personal data referred to in Number 14.

Number 17 defines the notion of "Health information". These are among the special categories of personal data referred to in Number 14.

Number 18 defines the notion of "international organization".

Number 19 defines the concept of "consent", whose scope and conditions are regulated in Article 4. Depending on the procedure in Article 46 Number 17 of the

German Federal Data Protection Act of June 30, 2017 (BGBl. I page 2097), the definition of consent from Regulation (EU) 2016/679 is used.

Number 20 defines the notion of "non-institutional person".

Number 21 and 22 define the concepts of "public authorities" and "non-public authorities". The definitions are used from Article 2 paragraphs 1, 2 and 4 of the German Federal Data Protection Act. The definition of public authorities has been supplemented by point (c) to make it clear that not only domestic public authorities, but also those of other Member States of the European Union are covered by the definition and, in principle, a transfer of personal data to them is possible if there is a legal basis. This corresponds to the target provision of Article 1 paragraph 2 (b) of Directive 2016/680 (EU). Non-public bodies, who are responsible for the sovereign tasks of the public administration, are public bodies. These include, for example, doctors with a contract who work in prisons. Also, free carriers of the criminal offender’s assistance can, in individual cases, for example, if they carry out a perpetrator-victim-compensation (Article 46a StGB, Article 155a StPO), also perform sovereign tasks of the public administration.

On Article 3 **Principles of data processing**

Article 3 paragraph 1 and 2 essentially correspond to Article 2 paragraph 1 and 2 JVollzDSG SH in the previous version.

Paragraph 1 emphasizes the right of prisoners and other interested persons to informational self-determination by this law or any other legislation adopted based on a law.

The target provision in paragraph 2 calls for a careful balance between the interests of the judicial enforcement of data processing and the right of the data subjects to informational self-determination. Sentence 1 concerns the principle of data minimization and thus relates to Article 4 paragraph 1 (c) of Directive 2016/680 (EU). The possibilities of anonymization and pseudonymization listed in sentence 2 are suitable means of protecting the right to informational self-determination, provided that data must also be processed in compliance with the principle of data minimization. They must be used if the personal reference is not required for the specific purpose of the work.

In paragraph 3, Article 7 paragraph 1 of Directive 2016/680 (EU) is implemented. To facilitate the required distinction between fact-based and assessment-based data, an appropriate labelling will have to be carried out, if - as is often the case in prisons - this has not already become known from the data itself, to which category they shall be assigned. In these cases, separate labelling is dispensable.

Paragraph 4 implements Article 11 of the Directive (EU) 2016/680 and regulates the prohibition on automated individual decisions based on profiling. This safeguards the right of data subjects not to be subject to any decision to assess personal aspects concerning them which are based solely on automated processing and which have a detrimental legal effect on them or significantly affect them. Examples of adverse legal consequences can be the refusal of enforcement-opening measures, the arrangement of disciplinary measures against prisoners or a ban on visits. Internal intermediate determinations or interim evaluations, which are the result of automated processes, are not included.

On Article 4 **Admissibility of data processing, consent**

The first paragraph shall be without prejudice to Article 3 paragraph 1 of the JVollzDSG SH in the previous version and paragraph 8 corresponds to Article 3(3) of the JVollzDSG SH in the previous version.

Paragraph 1 is fundamental to the admissibility of the processing of data by the prison authorities and thus sets the rule of law and the jurisdiction of the Federal Constitutional Court following the principle of the reservation of the law. Paragraph 1 determines, as a sector-specific special provision, that the law enforcement authorities should store personal data, etc. only if this is expressly permitted or ordered for the scope of this law in another piece of legislation. The condition is that another piece of legislation explicitly refers to the processing of personal data of prisoners or other data subjects processed by law enforcement agencies. At the same time, Article 8 paragraph (1) of Directive 2016/680 (EU) is implemented, according to which a data processing must be carried out on a clear and precise legal basis (see recital 33 to Directive (EU) 2016/680).

Recital 35 to Directive 2016/680 (EU) indicates that a consent can be the basis of data processing, also within the scope of this Directive, if it is ensured that there is a genuine freedom of choice of the data subject. While the recital recognizes that such freedom of choice may be doubtful in situations where an authority may instruct or require the data subject to comply with a legal obligation. At the same time, however, situations are listed- also explicitly for the execution of sentences -, in which a data subject can consent to data processing. Even if, unlike in Regulation (EU) 2016/679, consent is not mentioned in Directive (EU) 2016/680 outside the recitals, it is appropriate as a legal basis for data processing. This is also in line with the evaluation of the federal legislator, who has created legal regulation for informed consent in Article 46, number 17 and in Article 51 of the German Federal Data Protection Act. A possible case of the consent of prisoners can be found in Article 47 paragraph 2.

Paragraph 2 corresponds in content to Article 51 paragraph 1 of the German Federal Data Protection Act. Here, Article 7 paragraph 1 of Regulation (EU) 2016/679 has editorial adjustments.

Paragraph 3 corresponds to Article 51 paragraph 2 of the German Federal Data Protection Act. Here, Article 7 paragraph 2 of Regulation (EU) 2016/679 is used.

Paragraph 4 corresponds to Article 51 paragraph 3 of the German Federal Data Protection Act. Here, Article 7 paragraph 3 of Regulation (EU) 2016/679 is used.

Paragraph 5 essentially corresponds to Article 51 paragraph 4 of the German Federal Data Protection Act. In this provision, the approach described in Article 4a paragraph 1 of the German Federal Data Protection Act is combined with the thoughts from Article 7 paragraph 4 of Regulation (EU) 2016/679. The provision states that the assessment of the effectiveness of consent must be based on the circumstances of the granting. The provision of the Federal Data Protection Act has been supplemented by the fact that in the circumstances of the granting within the scope of the local law, in particular the special situation of the deprivation of liberty is to be considered.

This includes a special power differential between those responsible for the data processing and the data subjects, in so far as this is a prisoner. A voluntary granting is, however, is to be assumed on a regular basis if that particular power gap does not materially affect the decision of the data subject, in particular if a legal or factual benefit is obtained for the data subjects or if the law enforcement authorities and the data subjects have similar interests.

Paragraph 6 corresponds to Article 51 paragraph 5 of the German Federal Data Protection Act, in which the scheme of Article 4a of the German Federal Data Protection Act "a.F." has been used. So, the provisions of Article 10 of Directive 2016/680 (EU) expressing the need for special protection of special categories of personal data are complied with.

Pursuant to paragraph 7, Regulation (EU) 2016/679 also maintains the principle that consent does not presuppose viability within the meaning of the civil-law provisions, but the actual ability of the data subject to understand it. This question is to be assessed on a case-by-case basis.

According to paragraph 8, the legal representatives enter (parents - Articles 1626 and 1629 BGB -, guardians - Article 1793 BGB -, supervisors - Article 1902 BGB - as far as this belongs to their task group, as well as caregivers - Article 1909 - as far as can be deduced from the text of the order) the rights of the prisoners represented

by them, if the prisoners do not possess the necessary discretion to make the decision and if this does not jeopardize the performance of enforcement duties. From the point of view of the prisoners concerned and the law enforcement system, legal representatives are third parties. However, their involvement can often be necessary for the fulfilment of the enforcement tasks. The provision therefore transmits the thoughts from Article 67 Juvenile Court Act (JGG) on the data protection provisions by which legal representatives are on an equal footing with the prisoners in respect of the said rights. The restriction that enforcement purposes must not be impaired serves to prevent abuse.

On Article 5 **Data Secrecy**

Article 5 is essentially the same as Article 4 JVollzDSG SH in the previous version.

The determination takes over the thoughts of Article 53 of the German Federal Data Protection Act. The determination standardizes the duty of persons engaged in law enforcement to maintain confidentiality, regardless of whether or not the referral to the processing of personal data constitutes the focal point of activity. What is decisive is the de facto possibility of access, so external persons, such as tradesmen and cleaning staff are also covered by this regime. In contrast to Article 5, Article 19 exists on the transfer of data to external parties by the law enforcement authorities.

According to paragraph 2, the data secrecy does not end with the termination of the activity and corresponds to Article 53 sentence 3 of the Federal Data Protection Act.

Section 2

Collection

On Article 6 **Admissibility of data collection**

The definition contains the basic rules for the admissibility of the collection of personal data by the law enforcement authorities.

Pursuant to paragraph 1, data collection is only permitted if it is necessary for enforceable purposes as defined in Article 2 Number 2.

Paragraph 2 considers the special vulnerability of special categories of personal data defined in Article 2 Number 14 - Article 10 of Directive (EU) 2016/680. The data is particularly sensitive. The data associated with this increased personality relevance, as the Federal Constitutional Court stressed (BVerfGE 115, 320,348), and the associated increased intensity of interventions in the personal rights of the data subjects only allows the processing of this data under the strict condition that these purposes are absolutely necessary. "Absolutely necessary" is a transfer of data if it is indispensable in the specific case for the achievement of the respective purpose.

On Article 7 **Collection of data from data subjects**

The provision regulates the collection of personal data from data subjects. Paragraph 1 essentially corresponds to Article 6 paragraph 1 JVollzDSG SH as amended and paragraph 2 to Article 6 paragraph 3 JVollzDSG SH as amended.

Paragraph 1 contains the principle of direct collection, which is collection of personal data as a matter of principle with the participation of the data subject. Thus, paragraph 1 is an immediate outflow of the fundamental right to informational self-determination, as the data subject should be able to know who is interested in their data.

Paragraph 2 sets out the conditions under which the collection of personal data is allowed even without knowledge, without the participation of the data subject, by way of exception. This is only permitted if there is no indication that predominant legitimate interests of the data subjects are affected. In this respect, balancing must take place. Examples of paragraph 2 include staff members' observation sheets for suicidal prisoners, for example, as well as workplace controls in open-air prison for day-release prisoners.

On Article 8 **Data collection on prisoners from third parties**

Article 8 uses Article 7 of the JVollzDSG in the previous version.

The provision in paragraph 1 regulates the conditions for the collection of personal data on prisoners being able to consent without their knowledge from third parties. For those who are unable to give informed consent, paragraph 2 provides for the collection of data from legal representatives.

The collection of data on prisoners from third parties intervenes in the rights of prisoners more than it would do in the case of collection from the data subjects themselves. For this reason, paragraph 1 binds this type of collection of data to strict requirements. The catalogue referred to in paragraph 1 is final. Reference to Article 6 is intended to ensure that its requirements are cumulative, i. e. for special categories of personal data, processing must be strictly necessary. In addition, the prerequisites of Article 7 paragraph 2 apply, since it is a collection of data without the knowledge of the data subject. If data collection from third parties is carried out with the knowledge of the prisoners, this is permitted provided that the prerequisites of Article 6 and an alternative from the catalogue listed in paragraph 1 apply.

Paragraph 2 extends the power of inquiry to include the possibility of collecting personal data on prisoners without their knowledge from their legal representatives if they do not have the necessary discretion to consent. Depending on the category of data, the cumulative requirements of Article 6 paragraph 2 must still apply to the particular category of personal data. In addition, the reference to Article 7 paragraph 2 makes it clear that - in view of the fact that it is a collection without the knowledge of the data subject - a case-by-case decision has to be taken with the legitimate interests of the prisoners.

Due to the fact that the collection of data by third parties without the prisoners' knowledge means greater interference with the legal status of the prisoners, paragraph 3 indicates that non-public authorities are required to provide information, otherwise the information is given voluntarily. This is the only way to ensure that the non-public bodies can decide under their own responsibility whether and to what extent they wish to provide information or not.

The provision implements Article 6 of Directive (EU) 2016/680 which provides for a

differentiation according to different categories of data subjects.

On Article 9 **Collection of data on persons who are not prisoners**

Article 9 largely corresponds to Article 8 JVollzDSG SH in the previous version and implements Article 6 of Directive (EU) 2016/680.

The provision regulates the collection of data on persons who are not prisoners, such as family members, friends or other related parties. In order to achieve enforcement purposes, it is indispensable to discuss with the prisoners their situation, their contacts and their interaction. Inevitably the personal data of other persons must also be mentioned.

Paragraph 1 allows both the collection from prisoners as well as the collection from third parties, or outside of law enforcement. In addition to Article 8, it contains a further breakthrough of the principle of direct collection among the data subjects but binds the collection to strict conditions. Due to the fact that the collection of data is absolutely necessary for the achievement of the enforcement purposes and at the same time a balancing with the legitimate interests of the data subject takes place, it is ensured that the interventions in the rights of third parties are proportionate.

Paragraph 2 corresponds to Article 8 paragraph 3.

Section 3

Storage and use, file management

On Article 10 **Storage and use**

Article 10 builds largely on Article 9 JVollzDSG SH in the previous version.

Paragraph 1 contains the principle of purpose for the storage and use of personal data after their permissible collection and also serves the implementation of the normalized necessity principle referred to in Article 8 paragraph 1 of Directive 2016/680 (EU). Based on that, a processing of personal data is permitted only to the extent necessary for the performance of the task of the competent law enforcement authority. The provision also includes the power of the judicial authorities to store and use the data collected for another enforcement purpose within the meaning of Article 2 point 2. This power is a prerequisite for a functioning prison, which must fulfil the legal tasks entrusted to it to secure the execution and treatment of the prisoners and to ensure safety in the institution. For example, personal data collected for reasons of safety and order in the institution has the same high relevance for the treatment of prisoners and could have also been collected for this enforcement purpose. The processing of data for this other enforcement purpose is proportionate and in accordance with the constitutional principle of hypothetical data revocation (Federal Constitutional Court, First Senate judgment of April 20, 2016 - 1 BvR 966/09, 1 BvR 1140/09, Mag. Jur. 284 et seq.) and Article 4 paragraph 2 of Directive (EU) 2016/680.

Paragraph 2 sets out, with a final catalogue, the conditions for the law enforcement authorities to store and use the personal data that may be collected for a purpose other than that for which they were collected.

Paragraph 3 regulates the storage and use of special categories of personal data within the meaning of Article 2, point 14. The provision serves the implementation of Article 10 of Directive (EU) 2016/680. This provides that the processing of data particularly worthy of protection is allowed only if it is strictly necessary and there are appropriate safeguards for the rights and freedoms of the data subject. Sentence 2 provides for an exception in favour of special categories of personal data which are subject to official or professional secrecy (in particular health data)

and have been given over to an official or professional function based on a duty to maintain secrecy.

Paragraph 4 restricts the storage and use of personal data of data subjects who are non-prisoners and serves to transpose Article 6 of Directive (EU) 2016/680, which distinguishes between different categories of data subjects.

Paragraph 5 takes into account the requirements of enforcement practice and corresponds to the previous version in JVollzDSG SH. Paragraph 5 is necessary because it is not always possible to ensure, with a relatively high level of expenditure, that a separation between required and unnecessary data is possible, in particular in the case of file-based storage of personal data. Only in the case of unjustifiable effort for the separation may, as an exception, such data also be stored that is not necessary for the specific purpose. As a barrier, however, the additional requirement must be observed that the justified interest of data subjects or third parties in their secrecy is obviously outweighing.

Paragraph 6 builds on Article 9 paragraph 6 JVollzDSG SH in the previous version. If, pursuant to sentence 1, personal data are stored or used exclusively for data protection control, data backup or to ensure the proper operation of a data processing system, this data is subject to a special purpose limitation. A purpose-altering use is therefore only permitted to avert a significant risk to public safety. Sentence 2 refers to the further processing of log data in automated data processing systems.

On Article 11 of the **File management**

Paragraph 1 regulates the management of records on prisoners.

Paragraph 2 corresponds to Article 10 of the JVollzDSG SH in the previous version. Sentence 1 shall be borne by the technical development and specifically allows the management of an electronic file. It thus forms the legal basis for this type of record-keeping in the law enforcement. According to sentence 2, a system for the electronic record-keeping can be determined by legal regulation.

Section 4

Transfer

On Article 12 **Transfer to public and non-public bodies**

Article 12 regulates the transfer of personal data to public and non-public bodies and builds largely on Article 11 of the JVollzDSG SH in the previous version.

Paragraph 1 contains the general legal basis for the transfer of personal data. Unlike the following paragraphs, it does not differentiate between transfer to public and private parties, purpose limitation and purpose modification, special categories of personal data and other personal data. In particular, paragraph 1 is the legal basis for the exchange of data between law enforcement in the case of transfers and transfers of prisoners or for other administrative operations involving several law enforcement authorities. This is particularly true for cross-border operations. The prerequisite is that the receiving authority of the data needs the data for the achievement of enforcement purposes. The term "enforcement purposes" is determined in Article 2, point 2. The requirement principle standardized in paragraph 1 serves to transpose Article 8 of Directive (EU) 2016/680 and must be interpreted in accordance with European Union law within its scope.

Paragraph 2 sets out cases in which a transfer of legally collected personal data to non-public bodies is admissible. The prerequisite is that the data is transferred for the purposes for which it was collected. In particular, the use of data by private third parties for enforcement purposes such as treatment, counselling, therapy, and educational measures outside the institution is thus addressed by Article 12 paragraph 2. Paragraph 2 Number 1 includes, among other things, the transfer of data to free sources of aid. Paragraph 2 number 2 (e) extends the existing national legislation to include the use of pre-discharge measures, the transition to freedom, debt settlement, dismissal, reintegration, follow-up care or voluntary residence. As a result, the regular measures taken in practice for the integration of prisoners are recorded in addition and a data transfer to non-public bodies is allowed in this respect.

The provisions of paragraphs 3, 4 and 5 rule out the cases in which the transfer purpose is different to the collection purpose. This concerns the difference between the conditions under which a transfer is permitted based on whether or not the

transfer is made to public (paragraphs 3 and 4) or non-public bodies (paragraph 5). It stipulates that the scope of the admissibility of the submission to public authorities is wider than that to non-public bodies.

Paragraph 3 is used for the implementation of Article 4 paragraph 2 and Article 9 paragraph 1, sentence 1 of Directive (EU) 2016/680 (Principles of data processing with a changing purpose) and in the scope of Europe must be interpreted in conformity with the rules. A "different statutory provision" within the meaning of paragraph 3 point 1 which allows the transfer of personal data to a public body in a meaningful way, may also be one that falls under Regulation (EU) 2016/679. This takes into account the fact that, depending on the purpose of the processing of the data, the various types of processing of the law enforcement may be subject to either Directive (EU) 680/2016 or Regulation (EU) 2016/679 on a case-by-case basis. In the latter case, there is a need for a statutory authorization to transfer data to the competent public authority. Data transfers for pardons referred to in paragraph 3 number 2 (b) is not subject to Union law. To this extent, the provision does not need to conform to European law. Transfers of data for the performance of tasks delegated by law to the service providers responsible for social benefits (paragraph 3 number 3 (d)), for Federal Army official actions relating to the taking-up and release of soldiers (paragraph 3, point 3 (f)), asylum or immigration measures (paragraph 3 number 3 (g)), to fulfil the tasks of the youth services (paragraph 3 number 3 (h)), or to carry out taxation (paragraph 3 number 3 (i)) fall under Regulation (EU) 2016/679 and not Directive (EU) 680/2016.

The transfer of data to public bodies for performance of the tasks of forensic outpatient clinics, for asylum legal measures, to fulfil the tasks of the youth welfare offices and for case conferences with the security authorities has been incorporated into law, in order to take into account the needs of the practice.

Paragraph 4 restricts the power of transmission of the law enforcement authorities in favour of pre-trial detainees and prisoners in the detention types referred to in the second sentence of Article 1 paragraph 2 because they are presumed innocent or ordered to be deprived of their liberty provisionally. Therefore, prior to the transfer, a balance must be made with the legitimate interest of the remand prisoners to exclude the transfer. Paragraph 4 is used for the implementation of Article 6 of Directive (EU) 680/2016 (distinction between different categories of data subjects) and is to be interpreted in accordance with European Union law in its scope.

Paragraph 5 is used for the implementation of Article 4 paragraph 2 and Article 9 paragraph 1, sentence 1 of Directive (EU) 680/2016 (Principles of purpose amendment) and is included in the scope of Europe and must be interpreted in conformity with the rules.

Due to the increased sensitivity of the specific categories of personal data, they may be transferred only in the exceptional cases mentioned enumeratively without the consent of the data subject referred to in paragraph 6, again differentiating between public (number 1) and non-public bodies (number 2). The possibility of transmission of special categories of legally collected personal data to forensic outpatient clinics for the purpose of treatment measures, the discharge preparation and after-care was inserted in addition to take into account the need of the practice. "Absolutely necessary", within the meaning of paragraph 6, is a transfer of data if it is indispensable for the respective purposes in a specific individual case.

Paragraph 7 takes into account the fact that, in the case of persons who are not prisoners, an intervention by the law enforcement authorities has particular weight in their right to informational self-determination. The reference in sentence 1 to paragraph 1 shall be construed in accordance with the constitution narrowly regarding the legal interests underlying it in Article 10 paragraph 2 number (4) to (6) or Article 16. The second sentence extends the power of transmission of the law enforcement authorities with the possibility of transmitting personal data of third parties in order to facilitate the search for and detention of escaped prisoners. This is a sector-specific regulation. By the legally transmittable data are usually only meant the communications of the name and address of the contact persons. Paragraph 7 is used for the implementation of Article 6 of Directive (EU) 680/2016 (distinction between different categories of data subjects) and is to be interpreted in accordance with European Union law in its scope.

Paragraph 8 takes into account the needs of law enforcement practices and provides a proportionate control in terms of the interests and rights of data subjects. Paragraph 8 is used for the implementation of Article 6 of Directive (EU) 680/2016 (distinction between different categories of data subjects) and is to be interpreted in accordance with European Union law in its scope.

Paragraph 9 makes it clear that the transmission of personal data is permitted only based on an explicit statutory requirement and the rest is to be omitted, whereby no distinction between public and non-public bodies shall take place.

On Article 13 **Safety-relevant findings**

Increasingly, the law enforcement is also understood as part of the security architecture of the countries. In particular the handling of extremist prisoners and prisoners involved in organized crime is a special challenge for the security authorities and the prison. The exchange of information with security authorities is essential to ensure the security of the law enforcement institutions in order to allow enforcement and integration planning tailored to individual prisoners and their needs in order to prevent and further radicalization and jeopardization of with the enforcement objective other prisoners to involve the security authorities in the release preparation if the threat persists. In particular, the detention of prisoners in another department, relocation of prisoners, participation in a deradicalization program, monitoring of visits, correspondence and telecommunications, as well as integration planning involving the security authorities, are noteworthy.

Articles 13 et seq. are to be read in connection with Articles 27 et seq. The latter allow law enforcement to identify the identity of prisoners. Building on this, Articles 13 et seq. specifically allow the exchange of data with the security authorities in order to obtain further information on the respective prisoners and, if necessary, to enable a correspondingly planned execution plan. In this respect, there is a combination consisting of identification of the identity, possible performance of a security inquiry and case conference in the case of continuing danger. In addition, there is the possibility of selective exchange of information pursuant to Articles 10 and 12.

Pursuant to paragraph 1, the law enforcement authorities shall examine, in accordance with Articles 14 and 15, whether security-relevant information is available on prisoners and persons outside the prison who seek access to the prisons. Paragraph 1 is to be understood as a programmatic task, above all for the law enforcement facilities, in the case of prisoners and non-institutional persons, a safety-related review in accordance with Articles 14 and 15 must always be carried out. It remains unaffected that Articles 14 and 15 can allow a refusal of a review, for example, if the security request is at the discretion of the law enforcement authorities. The concept of a non-institutional person is defined in Article 2, paragraph 20.

Paragraph 2 defines the concept of safety-relevant findings. Safety-relevant means namely knowledge about extremist, violence-oriented settings or contacts with such organizations, groups or individuals. The same applies to contacts with organized crime. The list is not exhaustive; safety-relevant may also be in connection with mental disorders of prisoners. The examination competence of the prisons is extended in the following Article 15 to the effect that according to paragraph 2 sentence 2, among non-institutional persons involved in the integration of prisoners, other findings on significant criminal convictions, an existing addiction problem or other circumstances significant for the assessment of the reliability of persons can be security relevant.

On Article 14 **Prisoner review**

Paragraph 1, sentence 1 gives the prison authorities the power to turn to the judicial and security authorities with a security question concerning prisoners, if actual evidence of, in a reasonable period of time, a threat or a danger to the security of the institution is attributable to prisoners.

The imminent danger establishes the threshold for the intrusion into the right to informational self-determination of the prisoner, which is connected with the security inquiry. The risk forecast must be supported with facts and should not be based on assumptions and general principles of experience. The "imminent threat" is a real risk in the legal sense. It is not the violation of the protection of the "institution safety" that must be threatening, but this must be a danger threatening ("risk of danger"). There must therefore be actual evidence of the emergence of a concrete threat to the security of the institution. The damage to the leading causal history need not be predictable with sufficient probability, if there are already certain facts in individual cases on an imminent threat to the security of the institution. It is sufficient that a concretized and foreseeable event is recognizable, from which the violation of the security of the institution could result. Based on the "impending danger" condition provided for in sentence 1, therefore, only relatively diffuse indications of possible dangers for a security inquiry are insufficient. The situation is often caused by a high level of ambivalence of the significance of individual observations. The events can remain in harmless contexts, but they can also the beginning of a process that leads to a risk. It is not sufficient for a safety inquiry in itself to know that a prisoner belongs to a fundamentalist understanding of religion. Due to the required imminent danger, a data transfer, in order to find out whether a danger exists in the first place, is excluded. The imminent danger must be attributable to the prisoner in the sense that he is "entangled" in the dangerous situation as a suspected disturber. In accordance with paragraph 1, sentence 1, it is at the discretion of the prison authorities ("may") to require information from judicial and security authorities when there is an imminent danger to the safety of the institution. The purpose of the security request and the related data transfers is the protection of the security of the institution from an impending danger. The security authorities include, for the purposes of determining, the police authorities of the Federation and the regions as well as the constitution protection authorities, the authorities of the regions, the Federal Intelligence Service and the Military Counterintelligence Service. The same applies to the appropriate security authorities in the Member

States of the European Union. Examples of judicial authorities are courts, the public prosecutor's offices or the Federal Office of Justice. In accordance with paragraph 1, sentence 2 number 1, the law enforcement authorities may particularly request an inquiry pursuant to Article 41 paragraph 1 number (1) of the Federal Central Criminal Register Act. In accordance with paragraph 1, sentence 2 number 2 and 3, safety-relevant findings of the police authorities of the Federation and the regions and of the national office for the protection of the constitution may also be requested. In accordance with the "double door" model of the data protection law, according to which an authorization is needed both for the reception of data as well as for data submission, paragraph 1, sentence 1 and 2 only give the authorization for a data request. Paragraph 1, sentence 3 substantiates the notion of imminent danger referred to in paragraph 1, sentence 1, that actual evidence may arise in the implementation, in particular from condemnations of the prisoners and from their behaviour. There are also convictions from criminal proceedings, that do not serve as basis for the current detention, and an enforcement behaviour at previous custodial sentences. On the other hand, according to the experience of the prison, an imminent threat to the security of the institution is, for example, rather remote from prisoners with a high basic age at the admission to prison, prisoners with a direct admission to prison and prisoners having only a short-term subsidiary penalty.

Paragraph 2 specifies the scope and the specific end of the safety request pursuant to paragraph 1, sentence 2 numbers 2 and 3. In that regard, the provision also has a concrete effect based on inquiries made by the police authorities of the Federation and the regions pursuant to paragraph 1 sentence 1.

Paragraph 3 regulates the security request related data transfer by the law enforcement authorities. The request made to the authorities referred to in paragraph 3 sentence 1 shall involve the personal data, in particular the secure identity data. Paragraph 3 should be read in connection with Article 27 to the extent that it enables the law enforcement authorities to identify the identity of prisoners. In addition to identity data, the known alias personalities, the estimated completion time and the file number of the decision underlying the enforcement should be shared, in order to allow the requested authorities an information. In the transmission of data referred to in paragraph 3, the strict purpose of the data transmission, the request for security-relevant knowledge, must be taken into account.

According to paragraph 4, the concerned authorities share with the law enforcement authorities their security-relevant findings on prisoners. The concept of "safety-relevant knowledge" is defined more precisely in Article 13 paragraph 2. For the police and the constitution protection authorities of the countries, this standard means an authorization to transmission of data to the respective law enforcement authorities. In the absence of legislative competence, the provision for authorities of other countries, the Federal government and the Member States of the European Union is to be understood as a mere program phrase, in this case, the power to transfer of data must come from the respective sectoral legislation.

Only when the requests referred to in paragraph 1, sentence 1 and paragraph 1 sentence 2 give hints about a specific threat to the security of the institution, it is at the discretion of the law enforcement authorities ("may") to request additional information or documents from the judicial and security authorities. As it is clear from the wording "additional", this is information that goes beyond the "safety-relevant knowledge" of paragraph 4. In relation to the unspecified judicial and security authorities, paragraph 5 justifies no transmission power. This must be regulated in the respective trade laws.

Paragraph 6 provides that the personal data is to be managed in separate files or file systems, that is to be processed and stored. The background is the special protection of this data that may contain sensitive information.

Paragraph 7 authorizes the law enforcement authorities to continue the processing of the knowledge gained within the framework of the security request for the purpose of law enforcement and integration planning. The data is necessary for the correctional facilities first and foremost to detect security risks on site, in order to be able to deal with them. However, if it turns out from a security request that there are prisoners with special radicalization tendencies or a special problem of violence, the institution must be put in a position, to detain the prisoners concerned in a safe place not only for the protection of third parties, but it also has to be allowed to use the findings in particular for the further enforcement and integration planning, not only to help the prisoners, but also to be able to face long-term security threats. An example is the arrangement of specific de-radicalization measures for the prisoners or the dealing with a problem of violence. It is the task of the law enforcement to protect the general public against further offenses by offering the prisoner who is classified as a dangerous a coordinated treatment program. To do this, the knowledge gained within the framework of the security request must be allowed to

be processed. The specifications for the deletion of data and other rights of the data subjects follow from the other provisions of the law.

On Article 15 **Review of non-institutional persons**

Paragraph 1, sentence 1 states the principle that non-institutional persons may only work in a law enforcement institution, if there are no safety concerns. The concept of the non-institutional person is defined in Article 2, number 20 as a person who is not in a service or employment relationship with the law enforcement authorities, does not work on behalf of any other authority and does not work as an organ of the administration of justice. As follows from the wording "should work in the institution", sentence 1 refers above all to cases in which third parties seek access to the prison for professional reasons. Craftsmen or merchants are examples of this. Examples of a non-professional activity are the completion of a voluntary internship or the activity within the framework of an honorary office. Honorary staff or employees of external organizations and associations are also subject to the regulation. A poorer status of non-institutional persons or even a concrete mistrust is not connected with it in any way, since the same applies to the own staff of the law enforcement. As a result, the non-institutional staff are on an equal footing with the institutional staff. If the person is in a service or employment relationship with the law enforcement authorities or if they are acting on behalf of another authority in the prison, the law builds on the assumption that there are no security concerns. Persons who are not in a service or employment relationship with the institution or the supervisory authority and visit the institution on behalf of another authority are, for example, probation officers or police officers and trainee teachers. Paragraph 1, sentence 2 makes it clear that for the normal case ("should") reliability testing is to be carried out. The reliability test shall be carried out to maintain the security of the institution. An exception to the rule to carry out a reliability test is therefore displayed whenever a threat to the security of the institution appears remote. Example of such non-institutional people are those who—because of their position and their long-time participation in the law enforcement—are well-known by the prison administration and the institution already has trust in them for good reasons. Other examples are the employees of private state-owned companies, applicants who come to interviews to a prison or representatives of companies that are present there for contract negotiations. The reliability testing has to be carried out with the consent of the data subject. Therefore, their previously granted consent is needed. In order to enable an informed decision of the person concerned the reason for the reliability testing, its potential scope and the possible impact of the refused consent shall be shared in particular. Paragraph 1, sentence 3 gives the law enforcement authorities the power to request personal information. This includes the power for the

transmission of such information that is necessary for the purposes of a reliability check by the police and constitutional protection authorities, such as, in particular, the identity data of the non-institutional person. The request to third-party authorities is at the discretion of the law enforcement authorities ("may"). In the case of the discretionary decision and the request, the strict purpose of the reliability testing—to ensure the safety of the institution—must be taken into account. Paragraph 1, sentence 3 only gives power to data request and transfer of the information that is necessary for this. In accordance with the "double door" model of data protection, the power of the third-party authorities for data transmission to the prison authorities shall come from their respective sectoral legislation. Paragraph 1 sentence 4 substantiates the proportionality principle and declares that in urgent cases, the supervision of the non-institutional person shall take the place of the reliability testing. This also may be departed from in exceptional cases ("should"), if a threat to the security of the institution appears remote, for example, because the person concerned is known by the institution staff personally as always reliable with a view to security issues.

Paragraph 2 specifies the principle of proportionality for the discretionary decision about data query under paragraph 1, sentence 3. Based on that, a data exchange can be waived if, by virtue of the event, the nature, extent or duration of the stay or the activities in the institution the danger to the security of the institution is remote. The intervention by the data exchange in the fundamental right to informational self-determination of the non-institutional person is to be evaluated in this respect considering the danger for the safety of the institution, which is to be predicted prognostically. It must be taken into account, for example, whether the non-institutional person has contact with prisoners and, in the case of volunteers, with which specific offer do they come to the institution. In an unclear situation, the data query may be continued, since in this case a danger to the security of the institution is not excluded as remote. However, it is important to bear in mind that a reliability test of the law enforcement authorities remains unaffected apart from paragraph 2.

Paragraph 3 concerns admission to visit prisoners and the prison. The latter includes, for example, measures of rehabilitation and public relations work, such as the institutional visit, in order to attend a theatrical event of prisoners. Unlike in the case of non-institutional persons, it is not only data retrieval by third-party authorities that is subject to the discretion of the law enforcement authorities ("may") but also the reliability testing as such. In the context of the discretionary decision, the fundamental rights positions concerned are to be taken into account, in the case

of a family visit in particular the fundamental right under Article 6 of the Basic Law and the resocialization objective resulting from the prisoners' personal rights. It is to be taken into account to the extent that the reliability testing can have a deterrent effect. The discretionary decision for a reliability testing of prison visitors requires that there is actual evidence of an imminent danger to the security of the institution. The hazard prediction must therefore be supported by fact and should not be based on assumptions and general principles of experience. The "imminent threat" is a real risk in the legal sense. It is not the violation of the protection of the "institution safety" that must be threatening, but this must be a danger threatening ("risk of danger"). Actual evidence of an imminent danger to the security of the institution may, in particular, be due to the fact that there is safety-relevant knowledge about a prisoner who should be visited. The threat shall therefore not necessarily be from the visitors themselves. In that regard, the provision is systematically related to the third sentence of paragraph 3. Paragraph 3 revolves around the 'rule - exception relation' of paragraphs 1 and 2 in that the threat must be positively established before it comes to the reliability test and the intervening in the rights of the people concerned; these are not omitted until a danger to the safety of the institution can be ruled out as remote. The background of the control system is that the access to a law enforcement institution by non-institutional persons in order to perform activities in order to perform activities there is usually based on a voluntary decision. The activity performed in the institution for professional reasons, in particular, is also a possibility to particularly far-reaching insights in the processes of the law enforcement institution and there is therefore an increased risk. On the other hand, in the case of prisoner visits pursuant to paragraph 3, fundamental rights positions of prisoners and those affected go beyond the fundamental right to informational self-determination (e.g. Article 6 of the Basic Law) and which de facto make a visit appear as not completely voluntary. Visits are carried out regularly and can be selective, confined to certain premises often with good monitoring, so that the safety of the institution is put to a comparatively small risk. The reliability testing of visitors has to be carried out with their consent. Therefore, their previously granted consent is needed. In order to enable an informed decision of the visitors, the reason for the reliability testing, its potential scope and the possible impact of the refused consent shall be shared in particular. Paragraph 3, sentence 2 refers to paragraph 1, sentence 3 and authorizes a query of data from third-party authorities. The data request is at the discretion of the prison authorities and is limited to the purpose of data transmission, the reliability testing. The transmission of data by the law enforcement authorities for the purpose of reliability testing should be limited usually to the identity data of the visitor. Paragraph 3 sentence 3 increases the

authorization for transmitting data to the police authorities and the constitutional protection authorities on the information whether and for what prisoners the admission to a visit is sought.

Paragraph 4 concretizes the principle of proportionality and excludes defenders, assistants, lawyers, notaries and persons and bodies privileged by law as part of the monitoring of the written correspondence of prisoners, from reliability testing within the framework of prisoner visits. The protected communication of the prisoners should not be affected by any deterrent effect of the reliability test during prisoner visits. In addition, the above-mentioned groups shall be excluded from a review based on their respective constitutional rights or their legal position.

Paragraph 5 sets out the consequences, if the reliability review is denied by the data subject or if there are safety-relevant findings. The person will not be granted access to the law enforcement institution or only with restrictions. In the decision the basic legal positions of those affected must be taken into account, including the fundamental rights of prisoners, the rehabilitation order of the law enforcement, as well as for family visits in particular the fundamental right under Article 6 GG (Basic Law). The relevant legal positions are to be considered with the identified imminent danger or threat to the security of the institution. The concept of "safety-relevant knowledge" in paragraph 5, sentence 1 refers to Article 13 paragraph 2. Paragraph 5 shows with the phrase " safety-relevant knowledge […] is known" that the power to reliability assessment referred to in paragraph 1 sentence 3 and paragraph 3 sentence 2 includes the authorization to receive relevant information from the requested authorities.

Paragraph 6 governs the repetition of the reliability testing. This must be carried out ("should") if there are new safety-relevant findings in accordance with Article 13 paragraph 2. The same applies in the event that five years have passed since the last background check. The need for a new security check to ensure the safety of the establishment is to be presented. The necessity principle set out in paragraph 6 is used for the implementation of Article 8 of Directive (EU) 2016/680 and is within the scope of Europe law and must be interpreted in conformity with the rules. The deletion of the data collected shall be governed by Article 59 f. The time of collection of data on non-institutional persons is essential for the control period in accordance with Article 59 paragraph 2 and therefore must be documented.

On Article 16 **Case conferences**

Article 16, Case conferences with the safety authorities. In contrast to punctual data exchange, this dynamic is inherent in the fact that the receiving agency is able to react to the exchanged information without delay and, in turn, to communicate the current state of information. The exchange of information builds here on each other and can then increase from the conference out in scope and depth. Case conferences are often not limited to the mere exchange of information. The goal is much more, to adjust the actions of the authorities involved and to agree on a common approach in the case. Case conferences are guiding for action for the concerned authorities. The information exchanged is the basis for the further operative procedure. The information exchanged is used directly to take action against the data subjects. Both the dynamics of the exchange of information within the framework of case conferences as well as its action guiding nature for the participating authorities justify an increased intervention depth compared to the punctual data exchange pursuant to Article 12. Article 16 shall be borne by the special intervention and creates clear legal regulation standards with qualified intervention thresholds for the transmission of data for case conferences with the police and constitution protection authorities of the Federation and the regions as well as the constitutional protection authorities of the regions and the Federal Office for the protection of the Constitution, with qualified engagement thresholds for the transmission of data. Article 16 distinguishes between case conferences with the police and constitution protection authorities of the Federation and the regions (paragraph 1), case conferences with the constitutional protection authorities of the Federation and the regions (paragraph 2) and case conferences with the participation of the police authorities of the Federation and the regions and the constitutional protection authorities of the Federation and the regions (paragraph 3) and sets out the conditions for this purpose alone. The standard is based insofar on the jurisdiction of the Federal Constitutional Court regarding the informational separation principle. Based on that, the regulations that enable the exchange of data of the police and intelligence services are subject to increased constitutional requirements, in terms of the fundamental right to informational self-determination. The data collection and data processing powers of the various authorities are tailored to the respective tasks and thus are limited, and this is of legal importance. The more different is the nature of the different types of duties, powers and responsibilities, the more important is the exchange of data (see BVerfG, judgment of the First Senate of April 24, 2013 - 1 BvR 1215/07).

Paragraph 1, sentence 1 authorizes the law enforcement authorities to the transfer of personal data to the police authorities of the Federation and the regions in the framework of case conferences. The convening of the case conference is at the discretion of the law enforcement authorities, as is clear from the wording "may". Clearly, it is emphasized that the subject of the transmission of data and the expected release date, the expected dismissal address as well as the implementation and integration plans and also special categories of personal data may be covered. The latter group of data is specified in Article 2, number 14. If biometric data is exchanged in order to uniquely identify a natural person (Article 2 number 14 (c)), Article 16 paragraph 1 expands the transmission powers under Article 27 paragraphs 3 and 4 as a special authorization norm. The prerequisite for data transmission is that the information was collected legally. This makes it clear that illegal data collection must lead to a deletion of the data and its further use in the framework of a case conference is excluded. Paragraph 1, sentence 1 sets out as the transmission threshold the actual evidence of the continuing danger of prisoners for the general public, a probable date of dismissal in not more than one year and the need of prevention of illegal acts that are of considerable importance. The conditions must be cumulative. A continuing danger of prisoners referred to in paragraph 1, sentence 1, number 1 is to be determined in the context of a risk prediction at the time of the decision. The forecast must be based on facts and not only on general experience records or mere assumptions. The requirement of continuing danger should have a far-reaching synchronism with the requirements of the management supervision (Article 68 of the Criminal Code). The case conference with the police authorities of the Federation and the regions referred to in paragraph 1, sentence 1, number 2 requires that the data subjects will be released from prison, in all probability, within a period of not more than one year. The enforcement planning at the time of the decision is crucial. The provision shall counteract the "policialisation" of the law enforcement. It shows the ratio referred to in paragraph 1, sentence 1, to enable an exchange with the police authorities and a co-ordinated approach with this, for the purpose of a coordinated discharge preparation. In addition, the enforcement planning by the law enforcement authorities remains, as it is also clarified in paragraph 5. Paragraph 1, sentence 1, number 3 shows that the exchange of information within the framework of the case conference on the prevention of illegal acts must be of considerable importance. The requirements of the risk forecast of number 1 shall be specified. There must be a risk that the prisoners commit further criminal offenses and not only illegal acts. Criminal offenses of considerable importance are, in particular, crimes as well as

serious offenses. The offense must be at least in the mid-level of criminality, severely disturbing the peace of law and be able to significantly diminish the sense of legal certainty of the population. What is decisive is the concrete case-by-case consideration. The risk of small-scale crime does not meet the requirements for a case conference in accordance with Article 16. Paragraph 1, sentence 2 allows a data transfer within the framework of a case conference to police federal and state authorities for the preparation of execution, demonstrations and transfers. The case conference, that are at the discretion of the law enforcement authority, does not serve here —unlike in sentence 1— the co-ordinated discharge preparation, but the police protection of the above-mentioned activities. In comparison to sentence 1, the limited purpose of the case conference is to be taken into account at the extent of the data submission. A prerequisite for a case conference pursuant to sentence 2 is the risk of escape, violence against persons or property of significant value, whose preservation is necessary in the public interest, self-injury or suicide. The risk forecast must be based on actual evidence. Mere experience and assumptions are inadequate. Paragraph 1, third sentence establishes that the probationary assistance and the pretrial supervisory authorities are to be involved in the case conferences for the preparation of discharge pursuant to sentence 1 as a rule ("should"). This will help to ensure that, in the context of the case conference, this takes into account a variety of assessments, especially those that are not in the original remit of police authorities, such as issues of social and professional reintegration. As an exception to the rule, a case conference without probationary assistance and the pretrial supervisory authorities may take place, for example, if predominantly highly sensitive data with a specific security reference is exchanged and will be discussed further. In the context of a discretionary decision by the law enforcement authorities, such a decision requires the special justification. Paragraph 1 sentence 4 authorizes the law -enforcement authorities to query and collect, under the conditions laid down in Article 16, paragraph 1, sentence 1 and 2 personal data from the police authorities of the Federation and the regions. The provision is intended to counteract any possible "imbalance" of the law enforcement and the police authorities, according to which, although a large amount of information from the law enforcement is transmitted to the security authorities, conversely, only a small amount of information is leaked from the security authorities to the law enforcement. Paragraph 1 sentence 4 gives law enforcement authorities the opportunity to collect personal information from Federal and State police forces in order to fulfil their legal mandate and enforcement objectives, in particular for prisoners who have proven to be persistently dangerous until recently.

In accordance with the "double door" model of data protection law, paragraph 1 sentence 4 only gives law enforcement power for the query and collection of data. The powers of the police authorities of the Federation and the regions for transmitting data must result from their respective sectoral legislation. If the data to be transmitted belongs to a special category of personal data (Article 2 number 14, the transfer to another public body is only permitted under the conditions of Article 10, paragraph 3, Article 12, paragraph 6, point 1. In accordance with Article 10 paragraph 3, the data usage must be absolutely necessary for the purposes referred to in Article 10 paragraph 2. In accordance with Article 10, paragraph 2, point 2, a purpose-changing usage of personal data is permitted if this is expressly permitted or ordered by legislation or rules. If the data to be transmitted belongs to a special category of personal data pursuant to Article 2 number 14, the transfer to the police authorities of the Federation and the regions is only allowed if it is absolutely necessary to fulfil the purpose. The same applies to the collection of such data from the police authorities by the law enforcement, Article 10 paragraph 3.

The first sentence of paragraph 2 authorizes the law enforcement authorities to the transfer of personal data to the constitution protection authorities of the Federation and the regions in the framework of case conferences. The convening of the case conference is at the discretion of the law enforcement authorities, as is clear from the wording "may". The first sentence of paragraph 2, because of its structure, is parallel to paragraph 1, so that it can largely be referenced for the above reasoning. In the thresholds for transmitting data, paragraph 2 deviates from the provisions of paragraph 1- Paragraph 2 takes into consideration the fact that the tasks of the police authorities of the Federation and the regions as security authorities and the tasks of the constitutional protection authorities of the Federation and the regions as domestic intelligence services (collection and evaluation of information) differ. Police authorities and constitution protection authorities are to be seen separately in accordance with the principle of separation of information, which prevents the uniform legal classification as "a Security Complex". Paragraph 2 reflects this by establishing powers for the transmission of data in the context of case conferences, which powers are specifically tailored to the constitutional protection offices. In accordance with paragraph 2, sentence 1, personal data, including data that is part of a special category, may be transferred to the constitutional protection authorities of the Federation and the regions if certain facts of the suspicion of aspirations in accordance with Article 10, paragraph 2, point 4 justify that there is the risk of occurrence of a related threat to the security of the institution or the achievement of

the enforcement objective in a reasonable period of time, and if it is absolutely necessary to prevent the above-mentioned risks. The conditions must be cumulative. With reference to Article 16 paragraph 2 sentence 1 number 1 on activities or efforts in accordance with Article 10, paragraph 2, point 4, above all, the unsafe activities or aspirations, through the use of force or targeted preparation for measures against the free democratic basic order or the security of the Federation or a state shall be taken into account. Ultimately, this means all efforts, that establish the scope of tasks of the constitutional protection offices. Examples are efforts from the field of political or religious extremism. The suspicion for such efforts must be based on "certain facts". Assumptions or general experience are inadequate. Paragraph 2, sentence 1(2) makes it clear that the mere suspicion of activities or endeavours, within the remit of the constitutional protection offices, is inadequate for a data transfer. Based on the activities or efforts, neither the occurrence of a threat to the security of the institution nor the achievement of the enforcement objective in a foreseeable period is there. Paragraph 2, sentence 1 number 2 is thus a real risk in the legal sense. On the contrary, an imminent danger ("danger of danger") for the safety of the institute or the achievement of one of the objectives of enforcement is presupposed. Not the damage to the protected property, but a threat to it must threaten to occur. As protective goods, paragraph 2, sentence 1, number 2 refers to the safety of the institution and the achievement of the objective of the enforcement. Starting from the enforcement purpose, to enable the prisoners to lead a life of social responsibility without criminal offenses in the future, for example, a data exchange with the constitutional protection agencies may take place, if as a result of overt radicalization rehabilitation success would not be observed. The danger for the object of protection "enforcement objective" or "safety of the institution" must threaten according to the standard "within a manageable period". It must therefore be a temporally foreseeable event. Only relatively diffuse clues for possible dangers, in which the events either remain in harmless contexts, or they can even be the beginning of a process that leads to a risk, are inadequate. The mere realization that a person is attracted to a fundamentalist understanding of religion is insufficient, for example, for the assumption of imminent danger (see BVerfG, ruling of the First Senate of April 20, 2016 - 1 BvR 966/09 -, recital 113), The exchange of personal data with the constitution protection authorities in order to find out if there is an imminent danger, is also insufficient. The impending danger is a prerequisite for the case conference in accordance with Article 16 paragraph 2. If there is a need for further clarification of the facts of the case, it must be done by the transmission of non-personal information. In accordance with paragraph 2, sentence 1, point 3, the transmission

of data to prevent a threat to the security of the institution or the achievement of the enforcement objective must be absolutely necessary, that is to say, in the sense of the norm in a concrete individual case it has to be indispensable. This is to be taken into account in the context of the discretionary decision of the law enforcement authorities and is opposed to standardized case conferences with the constitutional protection authorities. Since the constitutional protection authorities, unlike the police authorities, are not security authorities, the first sentence of paragraph 2 does not take over the one-year period until the sentence 1 sentence 1 point 2 is dismissed

Case conferences to exchange information with the constitutional protection authorities referred to in paragraph 2 are therefore possible during the entire enforcement. In accordance with paragraph 2, sentence 2, the probation assistance and the supervisory agencies should be involved in the case conference, provided that the dismissal of the prisoners takes place in probably not more than one year. This will help to ensure that, in the context of the case conference, a variety of assessments will be taken into consideration for the discharge preparation of the prisoners. To give an example, such information is not included in the original scope of the constitutional protection authorities, such as, for example, questions of social and professional reintegration. As an exception to the rule, a case conference may be held without probation assistance and supervisory agencies if predominantly highly sensitive data with a specific security reference is exchanged and will be discussed further. In the context of a discretionary decision by the law enforcement authorities, such a decision requires the special justification. Paragraph 2, sentence 3 authorizes the law enforcement authorities to query and collect the personal data from the constitutional protection offices of the Federation and the regions. The provision is intended to counteract any possible "imbalance" of the law enforcement and the constitutional protection authorities, according to which, although a large amount of information from the law enforcement is transmitted to the security authorities, conversely, only a small amount of information is leaked from the security authorities to the law enforcement. Paragraph 2, sentence 3 gives the prison authorities the possibility to collect personal information from the constitutional protection authorities of the Federation and the states, in order to fulfil their legal mandate and the enforcement purpose especially for prisoners who seem to be extremist dangerous. In accordance with the "double door" model of data protection law, paragraph 2 sentence 3 only gives law enforcement power for the query and collection of data. The powers of the constitutional protection authorities

of the Federation and the regions for transmitting data must result from their respective sectoral legislation.

Paragraph 3 authorizes law enforcement for simultaneous exchange of personal data with the police authorities of the Federation and the regions and with the constitution protection authorities of the Federation and the regions in the framework of case conferences. The convening of the case conference is at the discretion of the law enforcement authorities, as is clear from the wording "may". In the thresholds for transmitting data, paragraph 3 sentence 1 deviates from the provisions of paragraphs 1 and 2. Paragraph 3 contributes to the fact that the tasks of the police authorities of the Federation and the regions as security authorities and the tasks of the constitutional protection authorities of the federation and the regions as domestic intelligence services (collection and evaluation of information) differ; joint case conferences, however, are created for a dynamic exchange of information beyond the respective authority boundaries. The need for an exchange of information between security authorities with different tasks and, in particular, the exchange of data between the police and security authorities creates, based upon the jurisdiction of the federal constitutional court, an intervention of increased weight in basic law. This is increasingly true, if the information exchanged—as usual in a case conference—regularly concerns the authorities involved and thus the data subjects used for action vis-à-vis the operational application. In such a case the data exchange is permitted only in exceptional cases. A prerequisite for the overcoming of the informational separation principle is that access to and use of the data serves the protection of particularly important legal interests. A present danger for such protected goods is not to be seen as a barrier to intervention. The risk forecast must be backed by certain facts (see BVerfG, judgment of the First Senate of April 24, 2013 - 1 BvR 1215/07 -, paragraphs 112 et seq., 201 et seq.). Paragraph 3, sentence 1 numbers 1 to 3 substantiate the constitutional requirements to a data exchange under overcoming the informational separation principle and allow joint case conferences of law enforcement authorities, police authorities and constitutional protection authorities if there is a cumulatively present danger to life and limb, health or freedom of a person or things of significant value, whose preservation is necessary in the public interest, if the suspicion of activities or efforts in accordance with Article 10, paragraph 2, point 4 is justified and the exchange of information is absolutely necessary for security reasons. The risk forecast and the suspicion of activities and aspirations in accordance with Article 10, paragraph 2, point 4 must be fact-based. Assumptions and general experience are inadequate. A risk is present if of the impact of the harmful event has already begun

or if this impact is imminent directly or in the very near future with a probability bordering on certainty. The protected assets referred to in paragraph 3, sentence 1 number 1 shall be interpreted in accordance with the provisions of the general police law. With reference to Article 3 sentence 1 number 2 on activities or efforts in accordance with Article 10, paragraph 2, point 4, above all the unsafe activities or aspirations, through the use of force or targeted preparation for measures against the free democratic basic order or the security of the Federation or a state are taken into consideration. The exchange of information is, according to in paragraph 3, sentence 1 number 3, absolutely necessary to avert danger, if it is indispensable for this purpose in a particular case. The second sentence of paragraph 3, declares paragraph 2 sentence 2 to be applicable mutatis mutandis. Also, as part of joint case conferences with police authorities and constitutional protection authorities, probation assistance and supervisory agencies should therefore be involved, provided that the dismissal of the prisoners takes place in probably not more than one year. This will help to ensure that, in the context of the case conference, a variety of assessments will be taken into consideration for the discharge preparation of the prisoners. An example is such information that is not included in the original scope of the constitutional protection authorities, such as, for example, questions of social and professional reintegration. As an exception to the rule, a case conference without probationary assistance and the pretrial supervisory authorities may take place, for example, if predominantly highly sensitive data with a specific security reference is exchanged and will be discussed further. Paragraph 3 sentence 3 authorizes law enforcement authorities to query and collect the personal data of the constitutional protection offices of the Federation and the regions and the police authorities of the Federation and the regions in the framework of the joint case conference. The provision is intended to counteract any possible "imbalance" of the law enforcement and the security authorities, according to which, although a large amount of information from the law enforcement is transmitted to the security authorities, conversely, only a small amount of information is leaked from the security authorities to the law enforcement. Paragraph 3, third sentence, provides the law enforcement authorities with the possibility of collecting personal information from the Federal and regional constitutional protection authorities and the Federal and regional police forces in order to fulfil their legal mandate and the enforcement objective, in particular for prisoners who consider themselves to be extremist and at the same time create a present danger for particularly important protected goods. In accordance with the "double door" model of data protection law, paragraph 3 sentence 3 only gives law enforcement power for the query and collection of data. The powers of the constitutional protection authorities of the Federation and the

regions and the police authorities of the Federation and the regions for transmitting data must follow their respective sectoral legislation.

In accordance with Article 16 paragraph 4, the main results of the case conference are to be documented. The documentation must be accurate enough to make the data exchange and, where appropriate, laying down that a consensual approach was carried out in order to be able to understand in such a way that subsequent legal protection and a subsequent data protection control are possible.

Article 16 paragraph 5 makes it clear that the enforcement and integration planning remains with the law enforcement authorities. Paragraph 5 is to be read in a systematic connection with paragraphs 1 to 3. Paragraph 5 is intended to counteract a "policialisation" and "intelligence service nature" of the law enforcement. It is used for the clarification that the case conferences with police authorities and the constitution protection authorities do not question the rehabilitation assignment and its anchoring in the law enforcement authorities. The right to decide on the enforcement and integration planning lies with law enforcement and is not under any primacy or reservation of the security authorities. These are only involved in specific cases and in the context of case conferences to the extent, as it corresponds to their statutory tasks and the respective prerequisites for data transmission are fulfilled.

On Article 17 **Other admissibility requirements for data processing with the safety authorities**

With the ruling of April 20, 2016 concerning arrangements of the Federal criminal law, the Federal Constitutional Court grouped together, consolidated and further developed its case-law on data collection and dissemination of data, (see. BVerfG, ruling of the First Senate of April 20, 2016 - 1 BvR 966/09, paragraph 292). The new Article 17 implements the criterion of the hypothetical data revocation for the area of the law enforcement specified by the Federal Constitutional Court in the decision for the data exchange with the security authorities. The reason for this is the consideration that a data exchange does not only take place between the various security authorities of the Federation and the regions regularly, but also between the authorities of the law enforcement and the security authorities. The information exchanged was often collected through intensive monitoring measures, such as the intervention in the mail, postal and telecommunications secrecy, the monitoring of the detention areas of the prisoners, or the reading of found data carriers and mobile phones. Conversely, information is transmitted to the law enforcement authorities and further processed, which data was obtained by the security authorities based on sometimes serious interventions in basic rights. The Federal Constitutional Court differs in its above-mentioned ruling regarding the further use of collected data in accordance with the principles of purpose and the purpose of amendment. A further use of already collected data within the original purpose only comes by the same authority, within the framework of the same task and for the protection of the same legal interests considering how they were decisive factors for the data collection (see. BVerfG, paragraph 279). Since the data exchange with the security authorities is based on inter-agency knowledge, insofar the constitutional requirements of the purpose amendment must be observed. The background of the constitutional requirements for the intended change is that the encroachment on fundamental rights of the original collection of data is deepened by the data distribution and the new use of the information. It threatens the specific conditions which allowed the acquisition of information to be devalued. If the legislator allows the further use of data for purposes other than those of the original collection of the data (purpose change), it must thus ensure that the weight of intervention of the collection of data is also taken into account with regard to the new use. The authorization to change a purpose is to be measured on the principle of proportionality. The weight that is added in the framework of the balance, is oriented to the weight of the intervention on the part of data collection. A distinction is made

by the Federal Constitutional Court between intermediate risk facts and protected property on the one hand, and suspicion and criminal offense on the other hand. In any case, a change of purpose requires that the new use of the data serves the protection of legal interests or the detection of offenses of such weight that constitutionally could justify their re-establishment with comparably serious resources (principle of hypothetical data revocation). The prerequisites for a change of purpose are not always identical with those of a data collection, whereas regarding the required degree of concretization of the danger situation or the suspicion of a crime. It is constitutionally required, but it is usually also sufficient to the extent that the data provide a concrete approach (see BVerfG, cited above, paragraphs 286 et seq.). The legislator may then—in relation to the use of data by security authorities—allow a change of purpose of data in principle, if it is information that in some cases specific shows approaches to detect comparable serious offenses or to ward off threats, at least in the medium-term threats for comparably important legal interests such as those for whose protection the corresponding data collection is permitted (BVerfG, cited above, paragraph 290). This does not apply to information from living room monitoring or access to information technology systems. In view of the special intervention weight of these measures, for each new use of data as the data collection itself also by an urgent danger or a sufficiently substantiated risk must be justified on a case-by-case basis (BVerfG, paragraph 291). The constitutional principle of hypothetical data revocation is defined for the exchange of information with the security authorities in the new Article 17 as a general principle that is to be taken into account for the transfer of data to the safety authorities and the collection of data in the case from these— regardless of the intervention intensity of the original data collection. The standard structure is based on Article 12 of the new federal criminal law. Thus, for the petition, the minister of the interior should be taken into account by an approximation of the laws of the various authorities with security tasks. The perspective is also a far-reaching synchronous operation of the administration of law enforcement and security agencies during data exchange and on the question of the hypothetical data revocation.

Paragraph 1 adopts the provisions of the Federal Constitutional Court to the purpose of changing the transfer of personal data to safety authorities, and thus the principle of hypothetical data revocation is introduced into the Law Enforcement Data Protection Act (see BVerfG, recitals 288 to 290). The standard is to be read in connection with the competence standards for data exchange with the security authorities and justifies no transmission power in itself. Paragraph 1 takes over the

constitutional requirements in such a way that transmission of data to security authorities is only permissible if such serious crimes or misdemeanours may be prevented, detected or prosecuted or at least comparable strong legal interests may be protected in such a way that a comparison to the data collection of equivalent legal protection is ensured. In addition, it is necessary in each individual case to carry out concrete approaches for the prevention, detection or prosecution of criminal offenses or offenses or to defend against threats in a reasonable period of time. The principle of hypothetical data revocation is hereby introduced into the Law Enforcement Data Protection Act, without being limited to particularly intrusive measures. The term "security authorities" means the police authorities of the federal and state governments, the state offices and the Federal Office for the Protection of the Constitution as well as the Federal Intelligence Service and the military security service. The same applies to the appropriate security authorities in the Member States of the European Union. With the data transmission "for the purpose of risk prevention, for purposes of security, for prevention or prosecution of offenses, the prevention or prosecution of criminal offenses or for the purposes referred to in Article 10, paragraph 2, point 4", the entire activity of the security authorities is on the timeline, from the creation of the situation by the offices for the protection of the Constitution and the classic danger defence by the police authorities to the prosecution of criminal offenses and misdemeanours. The term "in individual cases, specific approaches for the prevention, detection or prosecution of criminal offences" remains behind the suspicion in the criminal law sense. This refers to a specific event in the individual case, for example, in the form of a specific investigative approach, which justifies the data transmission. A data transfer is excluded if it is "into the blue" and is only supported by the hope of knowledge. The term "in individual cases, specific approaches […] for the prevention of threats in a reasonable period of time […] for significant legal interests" excludes a data transfer "into the blue" and supported solely by the hope of knowledge as well. Independent evidence from the information available is much more required, that a dangerous situation could arise ("risk of danger"). It is sufficient that a specific and temporally foreseeable event is recognizable, from which the violation of a legal interest could result. The same applies if the individual behaviour of a person is the basis for the actual probability that in the foreseeable future breach of a legal interest occurs. The "in a reasonable period of impending danger" is a real risk in the sense of police law. A data transmission to the security authorities, to find out whether a danger exists, is nevertheless excluded. With the phrase "in comparison to the data collection of equivalent legal interest protection" normatively detects the weight of the basic legal intervention on the part of data transfer on the encroachment on

fundamental rights to the data collection. The "comparability" follows from the legal interest-related collection thresholds in the form of a "weighting class", which includes a legal interest above this threshold. In the case of information from a security measure, reference should be made to the interest on which the data collection was based. With information from a prosecution measure, further clarification is required of the offence to be clarified. If, for example, Article 24 of the JVollzDSG SH presupposes a present danger to life or limb to allow the opto-electrical monitoring in an arrest, random findings from such monitoring can be used to defend against a freedom risk. The defence of a freedom does not seem equal to averting the danger to life (as the original collection purpose) but is of a comparable weight with a view to the collection threshold of the nature of the action. Otherwise, for example, the use of such information for the prosecution of an offense against crime would count as a criminal offense. The concept of the legal right refers to individual objects of legal protection and universal legal interests. In particular, the legal interests are particularly significant individual rights, the life, the freedom, physical integrity or of sexual self-determination. Particularly significant universal legal interests are, for example, the protection of the safety of the Federal Republic of Germany or of a region or the protection of the free democratic basic order (see BVerfG, paragraph 100). The criterion of equivalent legal interest protection of data collection and data transmission to the security authorities, seems to be relatively unproblematic for the authorities of the law enforcement. Usually, the law enforcement acts permit data collection under conditions that are significantly reduced compared to the intervention thresholds of the police laws. For example, Article 34 of BremStVollzG allows monitoring of written correspondence already then, if this is necessary "for security reasons" or to ward off the "threat to the achievement of the enforcement objective". Since the intervention in basic law must be based on intervention in basic law of the data collection, and because the conditions of the collection of data have an effect in the data transfer, the comparatively low data collection thresholds of forwarding data to the security authorities must be taken into account. The transmission thresholds of Article 17 paragraph 1 ensure that there is no transmission of data to security authorities for general assistance with their responsibilities. A data transfer is inadmissible for the purpose that this is "necessary for the fulfilment of duties and the maintenance of public security" or because "facts suggest that the data are necessary for the performance of tasks" —according to the constitutional requirements (see BVerfG, paragraphs 293 et seq.). This is specifically important for example with a view to a data transmission in accordance with Article 10 paragraph 2 number(4) in conjunction with Article 12, paragraph 3, point 2(j), that already allows, in solation, a

data exchange to the constitutional protection offices, if this is necessary for fulfilling their tasks.

Paragraph 2 stipulates that the specifications for data transmission to the security authorities also apply if the law enforcement authorities receive information from these. In this respect, the requirements of the Federal Constitutional Court on the purpose-changing transmission of personal data by the security authorities apply. For the criterion of hypothetical data revocation, it is important to understand if data is to be collected "for the purpose of risk prevention, for purposes of security, prevention or prosecution of offenses or for the prevention or prosecution of criminal offenses". First and foremost, the collection of data by the security authorities for the purpose of ensuring the safety and security of the institution is addressed. The timeline covers the entire spectrum, from the prevention of the emergence of a danger situation to security and law enforcement. "Prevention" is the order of the judicial enforcement, to protect the general awareness against further criminal offences. Paragraph 2, similarly to paragraph 1, refers to the protection of individual and universal legal interests. In the framework of law enforcement, the legal interests in question regularly represent a high weight. Examples are the rehabilitation provision derived from the general personal rights of the prisoners and the social state principle, the ensuring of the safety of the institution, the protection of the general public from criminal offenses or the protection of the criminal procedure in the pre-trial detention. With the security of the institution in mind, important legal interests are life, freedom, physical integrity or sexual self-determination, in addition to the guarantee of a rehabilitation-promoting environment. Data exchange from the safety authorities to the law enforcement authorities should then be possible to a large extent. Paragraph 2 shall apply, as well as paragraph 1, only for personal data. If, on the part of the security authorities, information without personal reference is transmitted, for example, to assess a book, Article 17 does not apply.

Paragraph 3 takes into account the particular requirements of the Federal Constitutional Court on the purpose-changing usage of data that was collected through the use of technical means, in or out of homes and by covert interventions in information technology systems. Paragraph 3 relates only to paragraph 1 number 1 (b) but applies both for the receipt of information from the security authorities as well as for the transfer of information to the security authorities, since paragraph 2 refers to paragraph 1. The transfer of personal data that was collected by the use of technical means in or from homes, is in accordance with paragraph 3 number 1 in

the case of the existence of a risk only possible, if—as Article 13 paragraph 4 GG determined—there is an urgent danger in a particular case. Paragraph 3 number 1 means by protected goods the existence or safety of the Federation or of a region or the body, life or liberty of a person or property of significant value, the maintenance of which is required in the public interest. The protected goods correspond to the specifications of the general police law for the use of technical means in or out of homes and are to be construed accordingly (see paragraph 183). The prison cell does not belong to the scope of protection of Article 13 GG. Accordingly, no data is collected there through the "use of technical means in or out of homes" (see BVerfG, Chamber decision of May 30, 1996 - 2 BvR 727/94). The transmission of information obtained this way to the security authorities is not governed by paragraph 3, point 1. With regard to the equivalent legal interest protection of data collection and transmission of data it must, however, be noted that the respect of human dignity and in particular privacy and intimacy as the expression of the general personality rights is also displayed regarding the detention areas of prisoners. It is to be recognized that the separate cell for prisoners is usually the only remaining opportunity to gain a certain degree of privacy and being undisturbed (see BVerfG, chamber decision., paragraph 13 et seq.). Since the transmission of personal data collected using technical means in a detention room, do not fall under paragraph 3, point 1, the scope of the provision is very small. Paragraph 3 point 1 (in connection with paragraph 2) especially applies when it comes to the reception of the corresponding data by the security authorities. If, in a next step, such information is further transmitted from the prison to other security authorities, paragraph 3, number 1, is also relevant. The transfer of personal data obtained through a covert intervention in information technology systems, is under paragraph 3, number 2 only permitted when certain facts justify in any case the assumption that damage to the life, limb or freedom of a person or such goods of the general public happens within a manageable period of time in a way concretized at least in its own way, whose threat affects the foundations or the existence of the Federation or of a country, or the foundations of human existence. The risk event is a real risk that in the legal sense and takes the appropriate decisions of the Federal Constitutional Court (see BVerfG, recital 213). The protected interests correspond to those of the general police law for the covert intervention in information technology systems and should be interpreted accordingly. Subject to the provisions of paragraph 3, point 2 is data that was collected by the covert access to the telecommunication device of the person concerned has been obtained, in particular its hard disk. If mobile phones are confiscated and read, this may not be via hidden access to an information system

(see BVerfG, ruling of the Second Senate of March 02, 2006 - 2 BvR 2099/04 -, recitals 93 et seq.). Otherwise applies for reading, for example, via the Internet. The practical scope of application of paragraph 3, point 2 for the law enforcement may, therefore— comparable to the paragraph 3, point 1— be small. Paragraph 3 point 2 (in connection with paragraph 2) especially applies when it comes to the reception of the corresponding data by the security authorities. If, in a next step, such information is further transmitted from the prison to other security authorities, paragraph 3, number 2 is also relevant.

Paragraph 4 provides by its reference to the personal identification data exchange in accordance with Articles 28 and 35, paragraph 4, that the requirements of the purpose and the principle of hypothetical data revocation do not apply if the basic data of a person is to be used for identification purposes. This corresponds to the jurisdiction of the Federal Constitutional Court to query and use of simple basic data for the purpose of identification (see BVerfG, judgment of the First Senate of April 24, 2013 - 1 BvR 1215/07 -, paragraphs 193 et seq.). The use of data is marked here by the mere use of basic data and the purpose of identification in two ways, and the intervention weight of the data transmission is reduced accordingly. Additional data - such as "hits" for the identified person - are not covered by paragraph 4; insofar as it remains with the requirements of paragraphs 1 to 3.

On Article 18 **Responsibility for the transfer and method**

Article 12, paragraph 1, Sentence 1 JVollzDSG SH in the previous version; paragraph 6 in turn, agrees with Article 13 paragraph 1 JVollzDSG SH in the previous version.

Paragraph 1 transfers the responsibility for the examination of the admissibility of a transfer of personal data in principle to the communicating law enforcement authority.

In accordance with paragraph 2, sentence 1, in the case of a transfer at the request of a public body, however, this bears the responsibility, and must have a legal basis for the collection of data. In this case, sentence 2 regulates the procedure for examination of the admissibility of a transfer.

Paragraph 3 lays down the procedure at the request of a non-public authority so that the law enforcement authorities can carry out the necessary examination of the admissibility of a transfer of personal data.

Paragraph 4 and 5 are used for the implementation of Article 7 paragraph 2 of Directive 2016/680 (EU) with regard to the verification of the quality of the personal data. The restriction on the transfer of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the enforcement of criminal sanctions including the protection and the prevention of threats to public security referred to in paragraph 3 results from the scope of the Directive, in accordance with Article 1(1) of Directive 2016/680 (EU). Paragraph 5 only applies for the scope of the Directive (EU) 2016/680.

Paragraph 6 concerns the necessity principle. Typically, the transfer of personal data that can be assigned to a specific person to non-public bodies is not required. In order to protect the data subjects, this data must be pseudonymized. Pseudonymization is legally defined in Article 2 number 7. Only if the pseudonymization is against the fulfilment of the purpose of the transmission, pseudonymization is to be exceptionally omitted. The prisoner registration number is a practical tool in the prison system to meet the prisoners' interests in pseudonymization. For the processing of data on order (Article 24), paragraph 6 shall apply accordingly, pseudonymization shall be done even there. Even with the

use of telecommunications and media services for non-public bodies (Article 12, paragraph 2 number 2 (d)), the data is to be pseudonymized without exception.

Article 19 **Formal obligation to third parties**

Article 19 is in compliance with Article 14 paragraph 1 to 3 JVollzDSG SH in the previous version.

The provision complements Article 5 and ensures that employees of non-public bodies to whom the personal data of the law enforcement authorities is transmitted, are informed about their obligation to maintain secrecy and the conscientious fulfilment of their obligations. This includes in particular the obligation to observe secrecy toward third parties and the prohibition of processing or disclosing personal data for a purpose other than for the performance of tasks without authorization.

In accordance with Article 24 paragraph 8, Article 19 applies to the processing of data on order.

On Article 20 **Communication on prison conditions**

Article 20 is based largely on Article 15 JVollzDSG SH in the previous version.

Paragraph 1 regulates the extent to which law enforcement may give information about the prison conditions. In this case there is differentiation between public and non-public bodies. In the latter case, the interests of the prisoners shall explicitly be included in the examination. The non-governmental organizations need to present their interest credibly, such as representation of a demand and the intended further steps, such as judicial enforcement or enforcement of the title. The law enforcement authorities are under no obligation to check the legality of the measures proposed.

The provisions of paragraphs 2 and 3 rule on the information on people directly and indirectly affected by a criminal offense. Legal successors are also entitled to information. If public property is damaged in the context of the offense, the public sector is also to be seen as victim of a criminal offense. Paragraph 2 number 2 and 3 are aligned with Article 406 (d) paragraph 2 numbers 2 and 3 of the Code of Criminal Procedure and give affected persons the right to be informed about both initial and subsequent law enforcement loosening. This serves the protection of victims. It is important to note that the arrangements referred to in paragraph 2, point 3—as well as in Article 406d, paragraph 2 number 3 of the Code of Criminal Procedure—are to be regarded as an exception. This is also reflected in the differentiation in paragraph 3 that, for the cases referred to in paragraph 2, point 3, always standardizes the separate presentation of a legitimate interest and does not already assume this as for the case referred to in paragraph 2, point 2. The presentation of the legitimate interest must make clear why an exception exists and why could it not be satisfied through the initial communication from the interests of the injured party.

Paragraph 3 waives the presentation of a legitimate interest in the case of persons mentioned there. This is in view of the added evil or analogue to Article 395 of the Code of Criminal Procedure.

Paragraph 4 privileges public law claims. The public sector, because of its paramount importance for services of general interest in providing information on the discharge address or the financial circumstances of prisoners, is to be treated as a victim of a criminal offense (paragraph 2).

The special position of the prisoners on remand - they are considered innocent - and prisoners who are in a prison in accordance with Article 1 paragraph 1 number 2 is also to be taken into consideration in the context of the communication on their prison conditions to external bodies. Paragraph 5, therefore, states that in the event of a communication on prison conditions it may only be specified whether a person is in custody in the institution. Due to the presumption of innocence, the suspected victims or their legal successors will not receive any information.

Paragraph 6 requires a balance of interests between the interests of those entitled to be informed and of the prisoners. In the event of a failure to consult the prisoners, not only a communication, but also an indication of the content is to be transmitted.

Paragraph 7 takes into account the particular interests of the recipients and also serves the protection of victims.

Paragraph 8 regulates the documentation requirement and is used for transparency.

As, with regard to the permitted communications on prison conditions, there is a distinction between the personal data of different categories of data subjects, Article 20 also serves the implementation of Article 6 of Directive (EU) 2016/680.

On Article 21 **File transfer**

Article 21 essentially corresponds to Article 16 of the JVollzDSG in the previous version.

The provision contains a special arrangement for the transfer of files with a list of eligible public bodies for this purpose. Such file transfer is at the same time the transmission of all data contained in the file. This level requires a legal transmission power. This regulation does not cover the exercise of the right to information and access to documents of the prisoners by an appointed defence lawyer, lawyer, notary or an appointed defence lawyer, lawyer or notary (Articles 54, 55). Even in these cases, the submission of the file is permitted (Article 55 paragraph 3).

Paragraph 2 provides a balance of interests, provided that an inseparable combination of data exists. For special categories of personal data, a predominantly legitimate interests of the person concerned in the confidentiality of the data is assumed from the outset, so that a transfer by means of the file transfer and thus an act of file transfer is inadmissible. The storage use and transfer of the inextricably connected data of the person concerned or of third parties by the receiving public authority is not permitted.

As paragraph 2 makes a distinction between the personal data of different categories of affected people, this also serves the implementation of Article 6 of Directive (EU) 2016/680.

On Article 22 **Information and file inspection for scientific purposes**

Article 22 corresponds to Article 17 of the JVollzDSG SH in the previous version.

The provision regulates the conditions for the provision of information and file inspection to scientific research, and public bodies for scientific purposes.

Paragraph 1 corresponds, in modified form, to Article 186 of the Prison Act. Article 476 of the Code of Criminal Procedure in taken into consideration. However, while Article 476 of the Code of Criminal Procedure presupposes that the data is stored in files, the transmission possibility is extended to electronically stored data, considering the technical developments.

The transmission of personal data referred to in paragraph 1, sentence 2 can also take place by electronic means. The transfer of personal data to the addressees referred to in Article 22 is permitted in accordance with Article 476, paragraph 1, sentence 1, insofar as this is necessary for the implementation of certain scientific research (number 1), the use of anonymized data for this purpose is not possible or the anonymization is connected with a disproportionate expense (number 2) and the public interest in the research work significantly outweighs the legitimate interests of the person concerned in the exclusion of the transmission (number 3). In weighing pursuant to sentence 1 number 3, in the framework of the public interest the scientific interest in the research project shall be paid special attention. In personal terms, the recipients must be officials, or, for the public service particularly people who are obliged or people who are obliged to secrecy (see Article 476(3) of the Code of Criminal Procedure).

Paragraph 2 considers in the enforcement of the pre-trial detention and deprivation of liberty in accordance with Article 1 number 2 the presumption of innocence.

The rule corresponds to the previous Article 17 JVollzDSG SH and also uses the provisions of Article 4 paragraph 3 of Directive 2016/680 (EU).

On Article 23 **Inspection of a prisoner's personal records, health records and medical records**

In accordance with Article 8 paragraph 2 (d) of the European Convention for the prevention of torture and inhuman or degrading treatment or punishment Germany is a contracting party to the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (hereinafter referred to as the Committee) and provides all information required for the fulfilment of its task. At this, the Committee observes the provisions of national law which, according to the comments on the provisions of the Convention includes in particular the regulations of the data protection (see paragraph 64 of the explanatory report).

In line with the further comments in the explanatory report, that possible difficulties in this field should be resolved in the spirit of the mutual understanding and co-operation on which the Convention is based, the provision creates a legal basis to make available to the Committee the information necessary to carry out its task.

Article 23 provides for the members of the delegation of the committee that these inspections of prisoners' personal records, health records and medical records during a visit are to be granted as far as is strictly necessary. This follows a request made by the Committee in the year 2016 that measures must be taken to ensure that delegations will get an unlimited access to the personal and health records of prisoners. A transfer of files takes place exclusively in the context of the institution visits. Therefore, the files can only be viewed on-site by the members of the delegation to the committee. The granting of access to said files - in particular the health records and medical records with their special categories of personal data - will be granted to the extent necessary for the performance of the duties of the members of the delegation of the Committee. The right of access of the members of the Committee is subject to the principle of purpose and implements Article 10 of the Directive (EU) 2016/680. Both in the prisoner's personal health records and files as well as in the medical records are special categories of personal data (see Article 2 number 14 within the meaning of Directive 2016/680 (EU). The intervention in the right of prisoners to informational self-determination that is associated with the consultation is, especially in view of the nature of the data particularly worthy of protection, is not negligible, but it is proportionate with regard to the task and purpose. The members of the delegation have to be evaluated, as a particularly important task, the treatment of persons deprived of their liberty to make sure that

the protection against torture and other prohibited treatment is implemented. A delegation of the Committee acts in the course of the visit in an institution as follows: They will see a random selection from all existing files to look through them cursorily. If this gives rise to more exact demands, there will be discussions with the affected prisoners. In this way, the members of the visiting delegation get a realistic and well-founded picture of the current conditions within the institution. This is because the unhindered access to the entire file inventory with regard to the prisoners is required. A previous selection of files, for example, on the basis of whether or not the prisoners in the inspection have given their consent, would no longer lead to an unbiased selection of the sample. Such a choice would be susceptible to manipulation and not only by explicit or hidden threats against prisoners in case of consent, but also in terms of indirect manipulation, such as ambiguous or misleading representations of the tasks of the visiting delegation. The core task of the Committee as a result of the human rights guarantees in Europe is a control without cause, which also includes the comprehensive inspection of the file inventory on the prisoners. Finally, the said intervention in the informational self-determination aims to protect the rights of the data subjects, in order to protect prisoners from abuse and inappropriate treatment in prison. The members of the delegation are, under Article 11 of the European Convention for the prevention of torture and inhuman or degrading treatment or punishment, subject to confidentiality in connection with the information received; personal data may not be published without the expressed consent of the data subjects. The health records and medical records of the prisoners may only be inspected in the institution by members of the visiting delegation with the corresponding vocational training, i.e. medical expertise. In this particular constellation, the standardized access to files is compatible with the protection of fundamental rights of the prisoners in accordance with the provisions of Article 10 of Directive (EU) 2016/680.

The definition also covers that professional secret holders give the members of the visiting delegation with the appropriate professional expertise information and explanatory notes on the content of the health records and medical records.

Section 5

Special forms of data processing

On Article 24 **Data processing on order**

The definition is used for the implementation of Article 22 of Directive (EU) 2016/680. It is based on Article 62 of the Federal Data Protection.

In paragraph 2, the rules in Article 18 paragraph 1 of the JVollzDSG SH in the previous version are used.

Paragraph 3 implements Article 22 paragraph 1 of Directive (EU) 2016/680.

In paragraph 4, conditions for the entering into of subcontracted normalized processing conditions normalized and the provisions of Article 22 paragraph 2 of Directive (EU) 2016/680 apply. By the duty to communicate information in sentence 2, there shall be the opportunity to raise an objection against changes in relation to the involvement or the replacement of other processors.

In paragraph 5, in acquisition of elements from Article 28 paragraph 4 of Regulation (EU) 2016/679, a subcontractor is subject to the processor obligations.

In paragraph 6, the required content one of the order processing underlying agreement. These contents are taken from Article 22 paragraph 3 of Directive (EU) 2016/68, Article 28 paragraph 3 of Regulation (EU) 2016/679 and Section 11 (2) and (3) of the Federal Data Protection Act; Thus, in sentence 2 point 1, elements from Article 28 paragraph 3 (a) of Regulation (EU) 2016/679 and Article 11 paragraph 3 sentence 2 of the Federal Data Protection Act, in points 5 and 6, elements of Article 28 paragraph 3 (h) of Regulation (EU) 2016/679, point 7, elements of Article 28 paragraph 3 point d of Regulation (EU) 2016/679 and points 8 and 9 elements from Article 28 paragraph 3 points c and f of Regulation (EU) 2016/679. Paragraph 6, sentence 1 shall, in implementation of Article 22 paragraph 4 of the Directive (EU) also 2016/680 statements on the form of the agreement.

Paragraph 7 is used for the implementation of Article 22 paragraph 5 of Directive 2016/680 (EU).

In accordance with paragraph 8, the formal obligation pursuant to Article 19 of the processing of personal data in the order accordingly applies.

On Article 25 **Data Processing for the transfer of implementation tasks**

The provision lays down the conditions to the processing of personal data by public or non-public bodies outside the geographic and organizational area of the prison authorities which have tasks of enforcement for self-standing completion within the spatial and organizational area of the prison authorities were transferred or to be transferred. Standards for the transmission of the power for implementation tasks are located in the enforcement laws of the regions and also, for instance, in Article 155 paragraph 1 of the Prison Act.

As far as a transfer completion of tasks is allowed, there is a need in addition a legal basis for the processing of personal data for the purpose of carrying out the tasks assigned.

In contrast to the "processing of personal data on order" this is described as "function transfers" in the data protection legal terminology. This is generally assumed when the contractor has his own decision-making powers with regard to the type and the selection of personal data, who independently carries out the task entrusted to him during the transfer of functions, and the client is to settle and thus process the personal data in individual cases that are no longer able to or only partially can influence, so that only in the context of the contractually agreed upon a service is provided, which goes beyond the instruction-dependent technical processing of personal data, the contractor for the admissibility of the processing of personal data to fulfil tasks to be transferred responsible rights of use of the personal data for its own purposes and having a personal interest in the processing of personal data.

As a transfer of function, in particular the largely independent organization of the prisoner's work or care of the prisoners and their medical care, professional service or the involvement of private merchants for largely independent handling of the institutional purchase within the institution can be considered.

For the design of function transfers, paragraph 2 sets out rules on the selection of the contractor (sentence 1), the guarantee of data protection standards (sentence 2), the written or in an electronic format to be determined issuing the contract (sentence 3) to the object and scope of the task transfer on the necessity of the processing of personal data for the performance of tasks delegated and the formal

obligation of the staff to be employed for this purpose pursuant to Article 1 of the Law on Obligations (sentence 4). The design of this function transfer is sufficiently concrete. Sentence 5 sets out an obligation on the part of the client to check and regularly document the compliance with the data protection measures taken by contractors.

As far as the transferred implementation tasks to be done, this law referred to in paragraph 3 to the processing of personal data application applies. In case of the function transfer to external bodies for self-standing fulfilment outside of institutions, this is based on the processing of personal data in accordance with the provisions applicable for the external facilities.

On Article 26 **Common responsibility of law enforcement**

The definition is used for the implementation of Article 21 of Directive (EU) 2016/680. For the protection of the rights and freedoms of the data subjects, on the one hand, and the determination of the responsibility and liability of the participating law enforcement, on the other hand, there is a need for a clear allocation of responsibilities within the framework of the agreement.

On Article 27 **Data synchronization detection**

Article 27 uses Article 20 of JVollzDSG SH in the previous version.

The unambiguous clarification of the identity of a prisoner in the prison is necessary in order to exclude identity confusion and to prevent interference in the fundamental rights of innocent bystanders. In order to enable the prisoners in the future to lead a life without crime and social responsibility to the individual and his history, there is a need to tailor implementation planning to ensure there is no doubt about the identity. In addition, the unequivocally establishment of the identity of the prisoners is necessary to ensure the safety and security of the institution. Numerous measures to ensure the security of the institution, such as the review of the prisoners in accordance with Article 14 or the exchange of personal data with the safety authorities require that the identity of the person concerned is clarified beyond doubt. In addition, the collection of data on the identity of the prisoners, by the assurance of enforcement in particular about a possible search and seizure in the case of escape. It is also important to prevent erroneous dismissals. Finally, the prison staff will be allowed to identify all prisoners, so as to allow a smooth daily routine. Article 27 is available in a systematic relation to Article 28. Article 27 regulates the permissible personal identification of the identity of the prisoners. If doubts remain, there is a recognition of service data comparison with the state Office of Criminal Investigation, the Federal Criminal Police Office, or the Federal Office for Migration and Refugees on the basis of the information collected, Article 28.

Finally, paragraph 1 regulates the permissible personal identification for the collection of data of the prisoners. The data collection is for law enforcement purposes. In this respect it is Article 2 paragraph 2 of the law. A law enforcement purpose is for ensuring the safety of the institution. Another purpose of the data collection will determine the identity of the prisoners, at the end of the day, but with the above-mentioned purposes as a secondary purpose. From the wording "are […] permitted" means that the law enforcement authorities are not obliged to take the above measures. This is at their discretion. Official recognition measures are therefore not obligatorily part of the admission procedure. Since the detection of the interests of the measures referred to in paragraph 1 may be carried out "for law enforcement purposes", the discretionary decision can be based on a variety of reasons. At least the absorption of photo images should be allowed on a regular

basis, in order to allow a smooth implementation of everyday life. In addition, for example, escape attempts, which belong to a criminal organization or the length of the implementation period will be taken into account in the decision. A limit of prisoners with a certain minimum duration in the law enforcement is not created. In the context of the exercise of discretion, the principle of necessity has to be observed. The collection of data is permitted at any time of the enforcement. Particularly in the case of photo images is must be checked in the course of time whether they are still up-to-date (beard, hair growth). At least after the expiration of three years ago, the production of new photos may be justified. It follows from the nature of the rule of discretion and from the principle of proportionality that the measures must be examined, chosen and justified on a case-by-case basis. This includes conducting standardization for the enforcement discretion not from everyday life. The taking of photos referred to in paragraph 1, point 1, may be of the whole body or only individual parts of the body. According to the conventional definition, photographic images of their technical production are such images that cause a radiation source (light, heat or X-rays) by chemical changes on radiation-sensitive layers, so especially black and white and colour photography. Photo images are only "biometric data", if processed with special technical means. Consequently, photographs are not per se subject to the special regulations of biometric data, but only when they are used to derive from them physical or physiological or behavioural characteristics or to analyse them (see Schreiber in: Plath, BDSG/GDPR, 2. GDPR edition 2016, Article 4). The acceptance of finger and palm prints in accordance with paragraph 1(2) may also be digital, for example through a fingerprint scanner. The outer physical characteristics referred to in paragraph 1(3) also include tattoos. Measurements taken in accordance with paragraph 1(4), for example, include the size and weight of a prisoner. In addition, the field is governed by facial recognition, paragraph 1, point 4. A handwriting sample of a prisoner is governed by number 4. Paragraph 1(5) allows the collection of biometric characteristics. The physical biometric characteristics may include, for example, the form of the face, retina, voice, hand geometry or the vein structure. The biometric capture of characteristics of the face, eyes, hands or voice is a safe way to determine the identity of a person. It is easy to manage, only with a relatively small number of interventions and is therefore in security fields outside of the law enforcement already applied. Even if it is very sensitive personal data they can use to the extent necessary for the affected a total of a lower burden, since control measures more effective, faster and less stressful can be carried out at the same time. From the signature referred to in paragraph 1, point 6 is a behaviour characteristic of a person. The data may only be collected regarding the prisoners.

In this respect, the principle of proportionality applies. Article 27 allows for the collection of biometric data. In accordance with Article 2, number 16, biometric data is collected with special technical processes, and is personal data relating to the physical, physiological or behavioural characteristics of a natural person or confirming the unambiguous identification of this natural person, especially facial images or dactyloscopic data. The definition corresponds to Article 3 paragraph 13 of Directive (EU 2016/680 and is in accordance with European law and must be interpreted correctly. Biometric data to uniquely identify a natural person is special categories of personal data (Article 2 paragraph 14 section c), which is in the collection and further processing of this data must be taken into account. In accordance with Article 6, paragraph 2, any special categories of personal data are collected only if it is absolutely necessary for law enforcement purposes, that is to say, essential in a concrete individual case.

Paragraph 2 makes it clear that the data collected not only in paper form in the prisoner's personal files, but also in the form of (electronic) may be processed in personal file systems. This is to ensure that knowledge is only possible for the purposes listed below in the law. There are organizational measures and questions of engineering design, such as the separate storage in the prisoner's personal file.

Paragraph 3 regulates the use of collected data. Article 16 and thus the use of the identification data in the context of case conferences from the arrangements referred to in paragraph 3 remains unaffected. Paragraph 3(1) is without prejudice to the principle of earmarking and specifies that the data collected may not be used for the purposes for which it was collected. Paragraph 3(2) permits the use of the data for the purpose of identification of the escaped prisoners or otherwise without permission residing outside the institution within the framework of a search and arrest. Paragraph 3(3) permits the use of the data for the purpose of Article 10, paragraph 2, point 7, as well as to the identity statement in accordance with article 28. Included in the collected personal identification data for the particular category of personal data pursuant to Article 2 paragraph 14 point c, is its storage or use for purposes for which it was collected, without the consent of the data subjects, which is only permitted to the extent necessary for one of the purposes referred to in Article 10 paragraph 2; it is essential to apply Article 10 paragraph 3 here. In accordance with Article 10, paragraph 2, point 2 is a purpose changing the storage and use of personal data is permitted if this is expressly permitted by legislation or rules. The purpose of changing usage detection service spatial data in accordance

with Article 27, paragraph 3, point 2 and 3 must therefore be essential when it comes to data for the specific category of personal data.

Paragraph 4 governs the transmission of data collected in accordance with paragraph 1. The recipients of the data are described in the following paragraphs. Paragraph 4 number 1 is to be read in a context of paragraph 3, point 2 and concerns the appropriate receiving authorities in case of a search and arrest. Paragraph 4 number 2 is to be read in the context of paragraph 3, point 3. Paragraph 4(3) covers the case of the transmission of personal identification data collected at the request of a public body. Paragraph 4(3) is without prejudice to the principle of hypothetical data new uplift to the purpose and allows changing data transfer to a public body, at their request, if the new collection of the corresponding data by the requesting agency would be allowed in a specific case. Not explicitly listed in Article 27, paragraph 4 are the recipients of a data transfer operation for the purpose of identification in accordance with Article 27, paragraph 3, point 3 and Article 28. The receiving authorities and the power of transmission come directly from the standard text of Article 28. The same applies to the rule of Article 16. Included in the data to be collected in the particular category of personal data (Article 2 paragraph 14 point c is the transfer to another public body which is only permitted under the conditions of Article 10, paragraph 3, Article 12, paragraph 6, point 1). In accordance with Article 10 paragraph 3, the data usage for the purposes referred to in Article 10 paragraph 2 is absolutely necessary. In accordance with Article 10, paragraph 2, point 2 a purpose-changing usage of personal data is permitted if this is expressly permitted or ordered by legislation or rules. If the collected identification data belong to the special category of personal data pursuant to Article 2 paragraph 14 point c, the transfer to another public office is therefore only permitted if this is absolutely necessary for the fulfilment of the purpose.

Paragraph 5 governs when the collected data is to be deleted. This must be done without delay, which means without undue delay after the release of the prisoners from the prison. The reference to Article 59 shows, apart from a deletion if the data is still required for law enforcement purposes. Law enforcement purposes, for example, can then continue to exist, if a prisoner under probation supervision or under the leadership is discharged. A permanent storage for the implementation of scientific research projects or for statistical purposes, such as Article 59, is not covered by the referral. Such a use of the personal identification data is not covered by Article 27 paragraph 3 and thus ruled out from the outset. In the case of a persistent storage of personal identification data about the time of dismissal, the

control and deletion periods of Article 59 must be observed. Instead of a deletion of data, a restriction in the processing is also to be taken into consideration, such as the reference to Article 60. Also, in this case, the possible uses of Article 27 paragraph 3 must be taken into account by Article 60 and cannot be extended. The data are in accordance with Article 60 is restricted in its processing to the relevant requirements set forth in Article 60. The erasure of data is to be documented in the prisoner's personal files. The documentation must be accurate enough to allow any legal protection and privacy control. Paragraph 5 is used for the implementation of Article 4 paragraph 1 point e, Article 5 of Directive (EU) and within the scope of Directive 2016/680.

On Article 28 **Data synchronization detection**

The unambiguous clarification of the identity of the prisoner in the prison is necessary in order to exclude identity confusion and to prevent interference in the fundamental rights of innocent bystanders. In order to enable the prisoners in the future to lead a life without crime and social responsibility to the individual and his history, there is a need to tailor implementation planning to ensure there is no doubt about the identity. In addition, the unequivocally establishment of the identity of the prisoners is necessary to ensure the safety and security of the institution. Numerous measures to ensure the security of the institution, such as the review of the prisoners in accordance with Article 14 or the exchange of personal data with the safety authorities require that the identity of the person concerned is clarified beyond doubt. Data synchronization detection in accordance with Article 28 is based on the identified measures pursuant to Article 27. Data synchronization detection is the collection of personal identification data.

Paragraph 1, sentence 1 stipulates that official data detection in accordance with Article 27, as well as the data in accordance with Article 14 paragraph 3 may be transmitted if there is any doubt as to the identity of the prisoners and the transmission of data to establish the identity is required. The purpose of the data transmission is limited to the identification. The data may be transmitted to establish the identity, finally from Article 27 and Article 14 paragraph 3. Subsequently, only basic data such as last name, maiden name, first name, date of birth, gender, place of birth, country of birth, nationality, aliens, identity-based photographs, finger and palm prints, detected external physical characteristics, measurements, biometric features of fingers, hands, face, eyes, voice and the signed signature may be transferred. As a threshold for a data transfer, Article 28, paragraph 1, sentence 1 "doubts about the identity" of the prisoners applies. This is the standard to the jurisdiction of the Federal Constitutional Court, according to which a transmission of basic data solely for the purpose of identity is not to be precluded when it comes to individual queries and a concrete reason for the transmission of data (see BVerfG, ruling of the First Senate of April 24, 2013 - 1 BvR 1215/07 -, recitals 192 et seq.). The fact that the transmission of data for the identification must be "necessary", refers to the need for a sustained examination of the property transfer event in individual cases (see BVerfG, recital 194). As a recipient of the data transfer, Article 28, paragraph 1, sentence 1 mentions the State Office of Criminal Investigation. In accordance with paragraph 1, sentence 2 allows the State Office of Criminal

Investigation the comparison of the transmitted data for the purpose of identification of the prisoners and must report the outcome to the law enforcement authorities. In this respect, the standard acts as a standard of authority for the State Office of Criminal Investigation. It empowers both for data comparison as well as the communication of the result to the prison authorities for the purpose of identification. The use of the data transmitted by the second sentence of paragraph 1 is therefore limited to the identification of the prisoners. Article 28 (1) does not authorize any further exchange of information relating to investigation or action. In accordance with other provisions in this respect, there is a need for action. Included in the collected personal identification data for the particular category of personal data pursuant to Article 2 paragraph 14 point c, is its use for purposes for which it was collected, without the consent of the data subjects, which is only permitted to the extent necessary for one of the purposes referred to in Article 10 paragraph 2; it is essential to apply Article 10 paragraph 3 here). In accordance with Article 10, paragraph 2, point 2 is a purpose changing the storage and use of personal data is permitted if this is expressly permitted by legislation or rules. The purpose of changing usage detection service spatial data in accordance with Article 28 must therefore be essential when it comes to data for the specific category of personal data.

Paragraph 2 extends the list of authorities to which data is transmitted for the purpose of identification and a comparison of data may be requested of the Federal Criminal Police Office and of the Federal Office for Migration and Refugees. Due to Article 28 paragraph 2 of the legal system, a country must have the authority for the data synchronization and communication of the result of the data correction for the law enforcement from the respective trade law of the federal authorities.

On Article 29 **Use of optical-electrical equipment**

Article 29 is essentially the same as article 21 JVollzDSG SH in the previous version.

The general provision regulates the conditions for the use of opto-electrical devices (video surveillance) in or to the institutions. In Article 30 to Article 32, there will be special regulations for different local areas of an institution. The use of opto-electrical monitoring and surveillance equipment is a particularly intensive intervention in the informational right of self-determination, as the prisoners have no opportunity to escape these measures.

Paragraph 1 therefore expressly binds their use to a corresponding statutory provision. Also, in this context, the use is exclusively for reasons of security.

In this context, paragraph 2 offers a uniform concept within the respective institution and the continuation of the ongoing adaptation to changing conditions.

In accordance with paragraph 3, it is already planned to ensure that opto-electrical monitoring is only used for reasons of security and to the extent required. At the same time, it must be ensured that the prisoners still have areas in which they are located outside of an optol-electrical recording.

Paragraph 4 ensures that the prisoners have knowledge of the video surveillance. Since the prisoners come from all cultures and social strata and not all are able to understand the German language, it is necessary to ensure by means of both linguistic and non-linguistic indications that the prisoners are clearly aware of the fact and also of range, that is, the actual spatial extent. A general note that the opto-electrical monitoring, for example, extends to the entire institution grounds, is not enough.

Paragraph 5 sets out the admissibility of video surveillance in transport vehicles of law enforcement and thus contributes to a need of the law enforcement and technical equipment of the new prisoner transport vehicles. During the process of transportation, the constant and direct supervision of prisoners in the prisoner transport vehicles is possible by means of opto-electrical equipment. Also, this observation shall be subject to the provisions of paragraph 4 of Article 32,

paragraph 4, as well as an adequate consideration of elementary needs of the prisoners, according to the privacy required.

On Article 30 **Opto-electrical devices within the institution**

Article 30 largely corresponds to Article 20 JVollzDSG SH in the previous version.

In observation of the external borders of institutions, it can happen that even outside of the prison grounds there is opto-electrical monitoring. As far as this is publicly accessible spaces, these can be observed in exceptional cases. Here, the concerns of possibly affected third parties, the in-house law of the prison manager of the institute and the need to ensure the safety of the institution are to be weighed against each other in accordance with the standards specified in the regulation.

On Article 31 **Opto-electrical devices within the institution**

Article 31 is consistent with Article 23 JVollzDSG SH in the previous version.

For safety reasons, the determination allows the opto-electrical observation of rooms and open spaces within the institution. A major limitation is set out in Article 32.

On Article 32 **Opto-electrical devices within prison premises and rooms**

Article 32 corresponds to Article 24 of the JVollzDSG SH in the previous version.

Paragraph 1 makes it clear that opto-electrical monitoring in detention rooms and bedrooms is in principle inadmissible, as detention areas and rooms are the only retreat for the prisoners, and they should be entitled to unobserved privacy.

In accordance with paragraph 2, opto-electrical monitoring within a prison space or room is exceptionally permissible within the framework of an observation as a special security measure, as far as this on a case-by-case basis to defend against a present danger to life or limb to the observed prisoners is required. The observation by means of optical-electrical equipment can only be used in addition to a direct observation. Because of the strong interference with the right to informational self-determination, this requires an explicit written arrangement and justification.

Paragraph 3 provides that prisoners are informed about the fact of the observation and this must be visible for them.

Paragraph 4 carries the basic needs of the prisoners to preserve their privacy statement by particularly sensitive areas such as sanitary facilities may be exempted or through technical measures to ensure that these areas are not visible in the context of the observation on the monitor. For example, this may be achieved with adequate pixilation in varying degrees, which is possible and permissible. Only in exceptional cases when there is acute self-injury or suicide risk may in individual cases, full monitoring take place. This is also to be included and justified in the written arrangement. The provisions in this Regulation are based on the recommendations of the National Agency for the Prevention of Torture (Annual Report 2013 of the federal agency and the Commission of the National Agency for the prevention of torture, Page 27/28).

Paragraph 5, with its interruption rule, is the result of the principle of necessity, but on the other hand also serves to protect special relationships of trust. In the presence of third parties, it will not be necessary to carry out electronic monitoring on a regular basis. An observation is e.g. ruled out for talks of the prisoners with their defenders. Due to the short-term and foreseeable interruption, the institution is relieved. The sequel to the same purpose and still existing conditions is not that a

new arrangement is required.

On Article 33 **Storage of collected data via optical or acoustic devices documentation**

Article 33 largely uses Article 25 JVollzDSG SH in the previous version.

Paragraph 1 establishes that storage of the data collected by an opto-electrical device may be carried out only to the extent necessary to delete data collected and otherwise. As far as the necessity must be checked on a case-by-case basis, under the conditions referred to in paragraph 1, with a period of 48 hours. The reference to Article 60, paragraph 1, point 1 to 3 and 5 contains situations in which limitation of processing takes place instead of the deletion because the data for the above reasons are still needed.

According to paragraph 2, the data collected by Acoustic-Electronic Devices shall also be treated when stored in accordance with the data from an optical-electrical observation. This is all recorded by means of acoustic monitoring. This also includes data from telephone monitoring.

Paragraph 3 stipulates that an observation by means of opto-electrical equipment within the framework of special security measures will not be recorded. The recording is not necessarily due to the related purposes. In order to avoid posing a threat to the prisoners concerned, immediate action is required. A control based on a recording does not achieve this purpose (more).

Paragraph 4 serves to protect the core area of private life. It takes into account the special situation of prisoners. The core area is subject to expressions through sensations, thoughts, views and experiences of a highly personal nature. This also includes communication with people of the highest personal trust. There is an absolute ban on processing such data; in particular, it may not be stored. Preventive measures shall be taken to ensure that such processing is excluded. Nevertheless, should it be stored, this data shall be deleted immediately. Communications directly relating to criminal offenses are not protected from the core area of private life, even if they are also very personal. Discussing and planning the content of criminal offenses is not part of the core area of private life but has social correspondence. However, a very personal conversation does not break out of the core area of private life, as it can provide useful information for the investigation of crimes or dangers. Records or statements made in the dialog, for example, only the inner

impressions or feelings and not containing references to specific offenses, cannot be a Community reference that you expose a criminal behaviour, causes or motives. Despite offenses can also cover situations where individual just to admit a wrongdoing or its consequences, such as confession confidential conversations or conversations with a psychotherapist or a defender or defender of the maximum personal privacy, the State is absolutely withdrawn. Then, if a sufficient social relation consists in talks with persons of trust in another connection directly to the subject of crime (see BVerfG, ruling of the First Senate on 20.04.2016 - 1 BvR 966/09, recital 122 according to Juris).

Paragraph 5 is used for the data protection control and obliged to document the processing by means of optical-electrical or acoustic-electronic equipment.

On Article 34 **Read out of data save**

Article 34 builds in large parts on Article 26 JVollzDSG SH in the previous version.

Paragraph 1 concerns strict conditions permitting the reading of electronic data storage units, as well as electronic devices with data store, without permission were introduced in the institution. According to the current state of the art, these are especially mobile phones and smartphones. The purpose of reading out these data stores is primarily to clarify subcultural structures and prevent the forwarding or disclosure of data of the institution possibly stored thereon (e.g., images of security-related facilities). Although reading is not an interference with telecommunications secrecy, it interferes with the integrity and confidentiality of information technology systems. In view of the importance of the intervention, only the head of the institution is authorized to issue an order. Before reading, a balancing of the interest is required. The reasons must be based on concrete actual clues and in the arrangement of legal protection reasons stated in writing. The reading should only be carried out while respecting the rights of the person concerned and, as far as possible to restrict the content, knowledge of which is necessary to maintain the safety and order of the institution. In particular, it is absolutely protected, to prevent data from the area of private life being read.

Paragraph 2 allows further processing of the data collected in accordance with paragraph 1 for law enforcement purposes.

Paragraph 3 prohibits further processing of the data collected, if it concerns the core area of the private life of the prisoners or third parties and arranges its deletion.

Paragraph 4 requires prisoners to be informed at the time of admission that data stores are being read out if they are brought to the institution without authorization.

On Article 35 **Identification of non-institutional people**

Article 35 builds on Article 27 JVollzDSG SH in the previous version.

In order to guarantee the safety of the institution, namely to enable the control of visit forbidden and the prevention of leaking through the exchange of visitors with prisoners, under paragraph 1, to establish the identity, in addition to the demographics and the proof shall be furnished by the official proof of identity, subject to strict conditions for the possibility of the biometric registration of the above-mentioned characteristics of the non-institutional people. By these measures to establish the identity is the institution a legitimate authority within the meaning of Article 2 paragraph 2 of the Passport Act (PAuswG) and can therefore also be in accordance with section 1, paragraph 1, sentence 3 and 4 require the deposit of the ID. The biometric registration of the above-mentioned characteristics represents a significant intervention in the informational self-determination and must therefore be carried out in accordance with paragraph 1 2 only to the extent necessary to prevent an exchange of prisoners is absolutely necessary. Therefore, for example, is the capturing of the mentioned characteristics of female people entering an institution that housed in the only male prisoners are not allowed. The biometric registration of the above-mentioned characteristics is also reserved on a case-by-case basis. There must be no general biometric visit check carried out.

Paragraph 2 establishes a close earmarking of data collected in accordance with paragraph 1. A change is referred to in paragraph 2, point 2 only for prosecution of criminal offenses, and only to the extent necessary for the prosecution of criminal offenses.

Paragraph 3 ensures that in the informational right of self-determination of the person concerned to intervene only as long as absolutely necessary.

In accordance with paragraph 4, a recognition of service data alignment with regard to non-institutional people is also possible.

On Article 36 **Photo ID cards**

Article 36 corresponds to Article 28 of the JVollzDSG SH in the previous version.

Paragraph 1, sentence 1 authorizes to commit the institution, the prisoners, for reasons of security or public order of the institution, must show a valid photo ID. This also includes the production of photo ID cards, in the dismissal of the prisoners or their relocation, they are to be destroyed. Sentence 2 shall ensure that a photo identification in addition to the image only those data are stored for the maintenance of security and order of the institution are required.

Paragraph 2 requires the confiscation and destruction upon discharge or transfer of prisoners.

Section 6

Protection requirements

On Article 37 **Earmarking**

Article 37 uses Article 29 JVollzDSG SH in the previous version.

For the purposes of determining is a protective legislation, the purpose-bound dealing with personal data of the data subjects, even after transfer. This is a possible abuse of power.

The receiver who receives the data for other purposes may only store, use and transmit it, in as far as they also had it for these purposes. For the purpose of further processing of data by non-public bodies, sentence 2 sets out in addition as an additional restriction that the prison authorities have agreed to the further processing.

Sentence 3 is used for the implementation of Article 9 paragraph 3 of Directive (EU) 2016/680, which should be provided, that, if special conditions apply for the processing, the transmitting competent authority the recipients of the data indicating that the conditions apply and must be complied with.

On Article 38 **Protection requirements**

Article 38 builds on Article 30 of the JVollzDSG SH in the previous version.

The rule is used for the implementation of Article 4 paragraph 1 (f) of Directive 2016/680 (EU) that personal data must be processed in a way that ensures an adequate level of security of personal data. At the same time, determining the requirements of article 19 of Directive 2016/680 (EU), according to which the controller, taking into account the nature, scope, the circumstances and the purposes of the processing as well as the different probability of occurrence and the severity of the risks for the rights and freedoms of natural persons take appropriate technical and organizational measures.

Paragraph 1 regulates the safe handling of personal data in files and file systems, so as to prevent unauthorized access and use. For the nature and scope of the technical and organizational measures necessary for this purpose, the provisions of paragraph 1, sentence 2 refer to the directory of processing activities, data protection through technology design and privacy-friendly default settings as well as to the implementation of a privacy and data protection impact assessment at high risk for the good of the data subjects.

Paragraph 2 refers to handling staff and their access to personal data. Any member of staff may only use such personal data that he needs for the fulfilment of the tasks entrusted to him. These requirements resulting from the principle of necessity must be ensured by technical and organizational protective measures, for example in the case of storage of files.

In accordance with Article 11, paragraph 1 prisoner health records must be kept. Paragraph 3 obliges the prison authorities to safeguard these files because they contain data particularly worthy of protection, separated from other documents and secure against unauthorized access and unauthorized use. They are subject only to the access of the doctors and the staff of the medical service.

On Article 39 **Directory of processing activities**

The requirement that the previous legal data protection regulations of the country of procedure is in compliance with article 70 of the directories, Federal Data Protection Act and is used for the implementation of article 24 of Directive (EU) 2016/680. The provision obliges the prison authorities to produce a list of categories of data processing activities carried out with them. This directory is used mainly in the country or the Data Protection Officer, an overview of the data processing carried out at the respective law enforcement authority.

In paragraph 1, the information to be included in the directory is presented. The term "categories" of processing activities is clear that the directory is not on individual data processing activities, but on useful parts of the definable and categorize topics in the law enforcement data processing carried out. The sequence of numbers is the same as that referred to in paragraph 1 of Article 30 of Regulation (EU) 2016/679. This is the practicality in the creation of the processing directories by the prison authorities, the directories are in the scope of Regulation (EU) 2016/679 in the framework of its administrative activities (personnel and economic area).

Paragraph 2 is standardized so that the processor is a directory of all categories of processing has to lead, albeit to a lesser extent.

Paragraph 3 provides information on the format of the directory.

According to paragraph 4, the directory is made available to the Data Protection Officer on request.

On Article 40 **Data protection through technology design and privacy-friendly default settings**

The definition is used for the implementation of the provisions of Articles 19, 20 and 29 of Directive 2016/680 (EU), the requirements of the duties of the person responsible for data protection through technology, design and privacy-friendly default settings as well as to the safety of the processing.

Paragraph 1 corresponds to the provision in Article 64 paragraph 1 of the German Federal Data Protection Act. The paragraph is based on the idea that the necessity of measures to measure whether your effort is proportionate to the protection purpose.

Paragraph 2 accepts the request; the data protection model corresponds to the standard catalogue. Articles 19, 20 and 29 paragraph 1 of Directive 2016/680 (EU) by the prison authorities may require, at the time of the appropriations for the processing as well as at the time of processing of reasonable accommodation to meet the data protection principles, such as the effective implementation of data minimization, and to ensure that the statutory requirements are complied with and the rights of persons affected are protected. The precautions to be taken, the state of the art, the cost of implementation and the nature, scope, the circumstances and the purposes of the processing as well as the different probability of occurrence and the severity of the hazards associated with the processing for the good of the data subjects must be taken into account. The objectives of the standard warranty data protection model, which is taken from the catalogue of requirements, consistent with the requirements of Directive (EU) 2016/680 (see *Schlehahn*, DuD in 2018, 32, 36). In addition to Articles 19, 20 and 29 paragraph 1, it is also possible to assign Articles 4, 5, 8 to 14, 16 to 18, 22, 24, 25, 28, 30 and 31 of Directive 2016/680 (EU) to these goals. The implementation of the measures referred to in paragraph 2 any law-enforcement authority under its own responsibility. The data processing is carried out via electronic book-keeping and accounting system in the prisons, the implementation of the necessary organizational and technical measures on a regular basis by participating in this system must be fulfilled. For example, the system BASIS-Web all functions that are necessary for the implementation of the above-mentioned measures, in particular a complex system of roles and rights. The actual assignment of the rights and roles usually remains the task of the institution director.

Paragraph 3 is used for the implementation of Article 29 paragraph 2 of Directive 2016/680 (EU). Sentence 1 shall designate the objectives, in terms of automated processing operations carried out by the establishment of appropriate technical and organizational measures. In accordance with sentence 2, the purpose of data media control, memory control, user control and access control, in particular through the use of state-of-the-art encryption methods can be achieved.

Paragraph 4 implements Article 20 paragraph 2 of Directive (EU) 2016/680. It is important to ensure that only the personal data is processed by preferences, whose processing after the respective specific processing is needed.

Paragraph 5 essentially corresponds to the legal situation in the previous regional data protection laws. The provision requires the development of a security concept and the assessment of the probability and severity of the risks associated with the processing of the right to informational self-determination. In contrast to the previous legal situation, the template in line with the new terminology and the requirements of Article 27 of Directive 2016/680 (EU) will no longer schedule a preliminary check by the person in charge (as in Article 20 of Directive 95/46/EC). A preliminary check sees Directive (EU) 2016/680 and accordingly also the draft only at a high risk for the right to informational self-determination in the context of article 41 of the privacy and data protection impact assessment to be carried out. Nevertheless, the good practice an assessment of risks for the right to informational self-determination on the basis of a safety concept for processing operations be maintained below this threshold. In accordance with paragraph 5, the consequences of data processing systems, regardless of the requirements for privacy and data protection impact assessment in the context of a safety concept can be estimated. This will at the same time concern the requirements laid down in Article 20 paragraph 1 and Article 29 paragraph 1 of Directive 2016/680 (EU), according to which the responsible for processing the data processing with the probability and severity of the associated risks must be assessed and, on this basis, technical and organizational measures to be taken. Article 41 on the implementation of a comprehensive privacy and data protection impact assessment at high risk for the legal interests of data subjects shall remain unaffected.

On Article 41 **Privacy impact assessment at high risk**

The provision essentially corresponds to the provision in Article 67 of the German Federal Data Protection Act.

Paragraph 1 is used for the implementation of Article 27 of Directive (EU) 2016/680. Criteria for the decision as to whether the proposed processing qualifies as high or increased risk to the interests of data subjects, for example, mas include the type of data collection means used or the circle of persons authorized to access, and thus the intensity of the processing associated with the intervention measures in the sense of an overall assessment. It is important to note that the requirement of carrying out a privacy and data protection impact assessment after the entry into force of this Act is only applies to new processing systems or significant changes to existing systems.

Paragraph 2 adopts the sentence 2 of Article 35, paragraph 1, of the Regulation (EU) 2016/679 and paragraph 3 incorporates Article 35, paragraph 2 of Regulation (EU) 2016/679, which complements the provisions of Directive 2016/680 (EU).

Paragraph 4 sets out the content of the privacy and data protection impact assessment and specifies the general information contained in Article 27 paragraph 2 of Directive 2016/680 (EU) general information contained in Article 35 paragraph 7 of Regulation (EU) 2016/679.

Contrary to the provision in Article 67 of the German Federal Data Protection Act, this provision contains no obligation on the persons responsible for carrying out a review of whether the processing follows the stipulations from the privacy and data protection impact assessment. Such an obligation is not stated by Directive (EU) (2016/680).

On Article 42 **Logging**

The rule is used for the implementation of Article 25 of Directive (EU) 2016/680 and allows monitor the lawfulness of data processing operations.

Paragraph 1 lays down the implementation of Article 25, paragraph 1, sentence 1 of Directive (EU) 2016/680 which establishes an obligation to log certain data processing operations in automated processing systems. In addition to the requirements of Directive 2016/680 (EU), the catalogue in point 1 has been supplemented with the storage of data and, in point 6, with the limitation of the processing. The regulation covers, among other things, the logging of automated data transfers to interfaces of procedures to other procedures, as well as processing operations by the administrator. Also included is the logging of so-called "reading access" requests, where information from the processing system within the meaning of sentence 1 of Article 25, paragraph 1 of the Directive (EU) 2016/680 can be queried (see. *Herbst,* in: Kühling/büchner, DS-Gmos/Bdsg, Article 4 GDPR marg. 27; Schaffland/Wiltfang, GDPR/BDSG, Article 4 GDPR marg. 74; according to another view is the read-only access to a subset of the collection, see *Schild*, in: BeckOK data protection law, Article 4 GDPR marg. 47; *Ernst*, in: Paal/Pauly, DS-Gmos/BDSG, Article 4 GDPR marg. 28).

Paragraph 2 provides concrete guidelines for the contents of the logs. Number 57 of Directive 2016/680 (EU) indicate that the identity of the person who has accessed or disclosed personal information should be recorded and the justification for the processing operations can be derived therefrom. The logging read requests will be done from the year 2023 when calling the respective main tab in the Web-based procedure which is based on a differentiated rights and role concept for access authorization is provided. This concept allows conclusions to be drawn on the basis of a query or disclosure, and therefore satisfies the requirements of Article 25 of Directive 2016/680 (EU).

The first sentence of paragraph 3 deals with the restrictions of use for log data. In principle, the log data can only be used for the purposes of the data protection control, self-monitoring and maintaining data security. The logging serves to protect the right to informational self-determination and is a procedural safeguard that mitigates the interference with fundamental rights. Under confined conditions, the logs referred to in paragraph 3, sentence 2 are also processed for the prosecution

of criminal offenses or to initiate official legal or disciplinary legal measures in connection with a breach of data confidentiality and for the prosecution of illegal acts that are of considerable importance. The corresponding amendment of purpose is set out in Article 25, paragraph 2 of Directive (EU) 2016/680.

After the decision of the Court in Case C-553/07 (ruling of the Court of Justice May 7, 2009, C-553/07), log data shall be kept for a period of time allowing the data subjects to understand the lawfulness of the processing. By the ruling of the Federal Constitutional Court, (Constitutional Court, judgment of 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) technical and organizational measures are to be ensured for the log data or the data protection officer in a legible and evaluable way and the log shall provide sufficient information to the logging activity that has to be monitored. In light of the compensation function, the Supervisory Control fulfils its regular implementation of particular importance. The controls are to be carried out at reasonable intervals - the duration of which may not exceed two years, - (BVerfG, ruling of April 20, 2016, 1 BvR 966/09, 1 BvR 1140/09, recital 141). Paragraph 4 specifies that the log data shall not be deleted until after two years of its creation, for a more extensive control over the processing of operations.

Paragraph 5 specifies that the protocols must be made available to the Data Protection Officer for the purpose of data protection control. The rule implements Article 25, paragraph 3 of Directive (EU) 2016/680.

The provision shall become effective only at May 6, 2023, in accordance with Article 65, paragraph 2.

On Article 43 **Identification within the institution**

Article 43 is essentially the same as Article 31 JVollzDSG SH in the previous version.

The provision allows the identification of personal data referred to in paragraph 1 within narrow limits within the prison. One of the provisions of this law, which could be on contrary with the identification, is Article 10.

Special categories of personal data referred to in paragraph 2 may not be disclosed.

On Article 44 **Insights from supervision, monitoring and control measures**

Article 44 uses Article 32 of JVollzDSG SH in the previous version.

Findings from the monitoring measures shall be subject to a special protection because monitoring measures intervene in particularly sensitive way with the informational right of self-determination of the data subjects. Often, these findings arise from a permissible procedure in Article 10, paragraph 1 GG. The scope of protection provided by Article 10 of the Basic Law also includes the information and data processing processes, to the knowledge of protected communication, as well as the use of this knowledge (see BVerfGE 100, 313, 359). With each notice, recording and utilization of communication data as well as the evaluation of the content and any other use by the public authority a self-standing intervention in basic law (see BVerfGE 85, 386, 398, 100, 313, 366, 110, 33, 52 et seq.).

In order to ensure the protection of fundamental rights, in accordance with paragraph 1 processing only takes place with the consent of the prisoners or on the basis of the privileged purposes in paragraph 1, sentence 2 number 2 and 3. Abuse is to be prevented by special identification of sensitive data.

Paragraph 2 extends the privileged purposes for the specific interests of pre-trial detention and the types of detention referred to in Article 1 paragraph 1 (2).

As far as the core area of private life is concerned, processing of personal data referred to in paragraph 3 sentence 1 does not take place and therefore there are no logging or recording activities being done by the supervisory officials. Sentence 2 makes it clear that the core area of private life usually does not cover conversations about, or relating to, criminal offenses or activities. For a more detailed definition of the core area of private life, see Article 33, paragraph 4, sentence 4. Should, however, data have been stored, you are obliged to delete it immediately. The obligation laid down in paragraph 3 on deletion and the associated documentation requirement shall take into account the protection of fundamental rights and the observance of which is controllable.

Section 7

Special provisions for people with access to secret information

On article 45 **Those with access to secret information**

The definition is used for the implementation of article 10 of Directive (EU) 2016/680 and is in compliance with Article 33 JVollzDSG SH in the previous version.

In paragraph 1, persons working in and for the prisons that are subject to a statutory duty of confidentiality or their action requires a duty of confidentiality. The persons listed in paragraph 1, sentence 1 numbers 1 to 3 are subject to the obligation of confidentiality, sanctioned in accordance with Article 203 paragraph 1 of the Criminal Code. For these people as well as for the pastoral counsellors mentioned in paragraph 1 sentence 1 number 4, paragraph 1 prescribes the principle of secrecy among themselves as well as with the law enforcement authorities. This secrecy also covers their assistants and the persons working for them to practice their profession, but not in relation to those holding the secrets themselves.

Paragraph 2 obliges the institution to inform external professional secretaries in their commissioning on the powers of disclosure and their duties in connection with their execution. External physicians, psychologists, etc., who are not regularly involved in the treatment of prisoners, cannot be presumed to be familiar with the particular revelatory powers and obligations set forth in this Act. On the one hand, the duty of notification allows the therapists, their interaction with the prisoners and, on the other hand, according to avoid later complications, such as when the institution information to certain treatment results on the basis of Article 34.

On Article 46 **Disclosure obligation**

The definition is used for the implementation of article 10 of Directive (EU) 2016/680 and is broadly in line with article 34 JVollzDSG SH in the previous version.
According to paragraph 1, professional secrecy holders are required to disclose the personal data disclosed to them to the institute director or the head of the prison if danger to life or limb is present or threatens a severe crime.

In accordance with paragraph 2, state-approved social workers, as well as social pedagogues and social educators who work as servants in the justice have a further disclosure obligation beyond paragraph 1. They are part of the institute as a staff member and have no special trust relationship, as they typically occur outside of law enforcement. Therefore, they must already communicate their knowledge to the head of the institution if this is necessary for the purpose of its functioning.

Paragraph 3 facilitates the fulfilment of the disclosure obligation and professional secrecy obligation of those holding secrets outside of law enforcement. Since they are regularly in contact with those holding secrets within law enforcement via this communication method, faster and more effective information of the institution is to be expected on this communication channel. It is the task of the institution in this constellation, professional secrecy and professional secrecy obligations outside of law enforcement to inform about the disclosure, as it cannot be assumed that this information is known without such a knowledge of these special obligations.

The entire provision constitutes a justification standard for professional secrecy holders.

On Article 47 **Authority to disclose**

The definition is used for the implementation of article 10 of Directive (EU) 2016/680 and essentially corresponds to article 35 of the JVollzDSG SH in the previous version.

Regularly, it can be assumed that those holding secrets on the basis of their own expertise can assess the extent to which the personal data becomes known for law enforcement purposes even, taking into account the interests of the prisoners in confidentiality, when it is strictly necessary. Therefore, they can decide whether to give information to the institute director or the head of the prison. Here, too, it is up to the institution to inform those holding secrets working outside the prison about the authority granted here. The provision is also a justification of the previous standard.

In order to ensure an effective treatment of the prisoners, paragraph 2 constitutes a power of disclosure in the relationship of the professional secrecy holders and thus an exception to the obligation of secrecy under Article 33. In the case of the above-mentioned conditions, those holding secrets are entitled to mutual information. This is necessary in order to enable targeted treatment. The power of disclosure applies across the board. However, the right of disclosure to other professional secrecy holders, which is facilitated in comparison with paragraph (1), does not apply if the addressee of a communication also exercises other, in particular executive, tasks in the institution, otherwise the treatment-related protection of confidentiality would not be sufficiently ensured.

On Article 48 **Notification of prisoners about disclosures**

The definition is used for the implementation of Article 10 and Article 12 (2) of Directive (EU) 2016/680 and is broadly in line with Article 36 JVollzDSG SH in the previous version.

In order for the prisoners to be able to decide independently on the disclosure of information, they must be informed about the obligations of disclosure and the powers of disclosure of those holding secrets. For the exclusion of misunderstandings and proof of sufficient information, the briefings by those holding secrets must be made in writing prior to the survey.

As the responsible body, the institution must ensure that the prisoners are informed of the obligations of disclosure and the powers of disclosure of professional secret holders prior to the survey, in the event of the involvement of secret holders from outside the institution.

While the fundamental and abstract preliminary information of prisoners is regulated in paragraph 1, the first sentence of paragraph 2 prescribes the information for concrete disclosure, so that the prisoners become aware of the actual transfer of data.

On Article 49 **Earmarking of disclosed personal data, approval of disclosure recipients**

Article 49 corresponds to Article 37 of the JVollzDSG SH in the previous version.

Paragraph 1 sets out because of the seriousness of the intrusion on the right to informational self-determination with regard to the disclosure of personal data from a special relationship of trust the strict earmarking of the revealed data.

According to paragraph 2, the head of the establishment may generally determine which other staff may be informed.

On Article 50 **Access to data in case of emergency**

The definition is used for the implementation of Article 8 paragraph 1 of Directive (EU) 2016/680 and largely complies with Article 38 of JVollzDSG SH in the previous version.
The provision enables access to personal data in emergency situations and makes it clear that data protection regulations must not impede an emergency rescue. However, the provision of direct knowledge is limited to persons working in the prison, who then have to transfer them to the persons employed for the emergency rescue - generally non-institutional people.

Paragraph 2 expressly extends the rights and obligations under paragraph 1 to the personal data collected by those holding secrets.

By prohibiting any other use of the purpose and the obligation to provide the documentation required in paragraph 3 to prevent a risk of misuse.

Section 8

Rights of the data subjects

On Article 51 **General information for data processing**

The rule is used for the implementation of Article 13 paragraph 1 of Directive (EU) 2016/680. The law enforcement authorities have the duty to provide information to the data subjects regardless of the assertion of their rights. These information requirements can be met by the prison authorities in general terms. Data subjects are independent of the data processing in the specific case in an easily accessible way an overview of the processing purposes and an overview of their affected rights. As is apparent from recital 42 of Directive (EU) 2016/680, for example, this obligation can be met by providing appropriate information on a web page. For prisoners, this commitment can be met with general information being provided in written form when recording in prison.

On Article 52 Obligation to inform in data collection with knowledge of the data subjects

Article 52 corresponds with Article 6 paragraph 2 of JVollzDSG SH in the previous version.

This provision transfers the law enforcement authorities shall be responsible to inform the data subjects of the purposes for which the data is collected and be informed of their rights in connection to that. This is the only way they can, within the scope of its possibilities self-determined about the handling of your personal data, to influence or inform yourself. Through providing information to the prisoners on their rights, legal disadvantages can be avoided.

On Article 53 **Notification of data collection without the knowledge of the data subjects**

The definition is used for the implementation of Article 13 paragraph 2 of Directive (EU) 2016/680. In "special cases", the notification of the data subject must include more information. The special cases are not defined in Directive (EU) 2016/680 (EU). The recitals provide no additional information. In Article 13 paragraph 2 point d of Directive 2016/680 (EU) it is concluded that this is particularly the case, in which data on prisoners or other data subjects is collected without their knowledge. However, it is expected that a transfer of the data for other purposes than the original survey triggers a notification obligation, providing a deeper intervention in the right to informational self-determination is connected.

Paragraph 1 provides for a notification obligation on the part of the prison authorities without knowledge of the data subject, if personal data is collected or communicated. In these cases, in addition to the information referred to in Article 51, further information must be provided on the legal basis of the processing, the duration of the processing and the recipients.

Paragraph 2 allows knowledge in implementation of Article 13 paragraph 3 of Directive (EU) 2016/80 from the provision of the information referred to in paragraph 1. Paragraph 2 provides in accordance with the existing rules in the relevant data protection provisions of the law enforcement authorities (for example, Article 39 paragraph 1 of the JVollzDSG SH) a catalogue of exceptions to the notification obligation, which in Article 13 paragraph 3 of Directive (EU) 2016/680 has been expanded. The exceptions to the notification obligation correspond with the appropriate restrictions on the provision of information to the data subjects in Article 15 paragraph 1 of Directive (EU) 2016/680 (Article 54). The decision to postpone the notification, limit, or to refrain from any action that must comply with the principles of proportionality and must be preceded by a reasonable balance of interests. An exception to the notification obligation is justified if an overriding interest in the prevention of the risks is referred to in paragraph 2 and disadvantages in comparison to the information interests of the data subjects is given. If, due to the specific circumstances of the individual case information the secrecy interest outweighs the interest of the data subjects, a notification has to be given accordingly.

In accordance with paragraph 3, prior to the notification of the data subjects, consent of the designated public authorities must be obtained, so that the information current procedures of that State, such as investigations by the public prosecutor's office, are not at risk. Because of the advanced notification obligations and the consonance with the information obligations, the corresponding exception is already in the decision upon notification to the data subjects in accordance with the procedure necessary in order not to endanger the notification alone. The provision is in line with Recital 44 of Directive (EU) 2016/680, which makes it clear that a notification, information, correction or deletion of personal data or restriction of the processing can be omitted, in order not to jeopardize ongoing investigations. This also applies to information from news services, whose activities fall within the scope of Directive (EU) 2016/680 (see recital 14).

Paragraph 4 concerns the exclusion of notification to the data subjects under the regulations on the right to information in article 54(6). In the case of a limited notification to inform the data subjects. However, this does not apply if the granting of this information is a risk, a disadvantage or an impairment within the meaning of Article 53 paragraph 2. Notifications for the prisoners or other data subjects may therefore be omitted if already in the specific case of the notification high-level interests are at stake (see recital 44 of Directive (EU) 2016/680. In this case, in exceptional cases, a referral to the state commissioner for data protection and freedom of information is not permissible. Law enforcement authorities' documents are the reasons for the postponement, restrict or omission on the part of the notification referred to in paragraph 2.

On Article 54 **Right of access of the data subjects**

The provision lays down in implementation of Article 14 of Directive (EU) 2016/680 the right of access of prisoners and other data subjects. From this information right, Article 15 of Directive (EU) 2016/680 contains exceptions. Already Article 40 JVollzDSG SH provided information rights of the prisoners, which could be omitted under certain conditions.

In paragraph 1, sentence 1 sets the fundamental existence of a right of access. Sentence 2 expands the scope of information. The term "category" referred to in paragraphs 1 and 4 allows the law enforcement authorities a reasonable generalization of information relating to personal data being processed and the transfer recipients. The information referred to in paragraph 1 to the processed personal data, in the sense of a summary statement in an intelligible form. The data therefore does not need to be made in a form, the information about the type and manner of storage or visibility of the data for law enforcement agencies (in the sense of a copy). Similarly, the obligation to indicate the information available about the data source is not that the identity of individuals or even confidential information must be disclosed. The law enforcement must register with the indication of the personal data, the subject-matter of processing operations at the end of the day, the legislative goal for the affected person to create awareness about the extent and nature of the processed data and enable it, on the basis of this information to assess whether the processing is legitimate and - if there is any doubt this are concerned - if applicable, the assertion of further rights to this information.

Paragraph 2 is based on Article 19 paragraph 2 and Article 33 paragraph 2 sentence 1 of the German Federal Data Protection Law in the version promulgated on January 14, 2003 (BGBl. I p. 66), the last by Article 10 paragraph 2 of the law of October 31, 2017 (BGBl. I p. 3618) has been changed. The expansion of the existing legal situation, however, to ensure that the responsible through appropriate technical and organizational measures to use the data for other purposes is excluded. When calculating the amount of effort, the person responsible for the existing technical possibilities, Locked and archived data of the data subjects in the framework of the provision of information to make available, to be taken into account. The data will be stored solely on the basis of retention requirements, the processing of the data is to be limited.

An information injunction, in accordance with paragraph 3 of this article shall not be issued in those cases in which the data subjects does not provide sufficiently concrete information, with which the processed data can be identified. If, for example, a visitor does not specify which prisoner he or she has visited, the obligation to provide information would result in a disproportionate effort on the part of the enforcement authority

Paragraph 4, by referring to Article 53 paragraph 2 and 3, adopts the exclusion grounds on which notification may be waived, including the provision of information. Depending on the scope of the affected interests, the information may be fully or partially restricted. The limitations correspond to Article 15 paragraph 1 and recital 44 of Directive (EU) 2016/680.

Paragraph 5 Sentences 1 and 2 shall be used for the implementation of Article 15 paragraph 3 sentences 1 and 2 of Directive (EU) 2016/680. Under the condition of sentence 2 shall be presented to the prison authorities granted the right to make a request for information completely unanswered. According to sentence 3, reasons must be given for not providing the information to the prisoners or other data subjects the review of not providing the information.

In paragraph 6, sentence 1 provides for the implementation of Article 17 of Directive (EU) 2016/680 as a new procedure for effective protection of the rights of persons affected by the review of the processing activities by the State Ombudsman or the commissioner for data protection and freedom of information in a special procedure. In accordance with paragraph 6, sentence 1 shall enter into force or the country representative for data protection and freedom of information in the rights of the data subjects. The law enforcement authorities point out to the persons concerned that they can exercise their right of access through the State Commissioner for Data Protection and Freedom of Information, and to the possibility of claiming judicial protection (sentence 7). If the data subjects make use of their right, the data protection or freedom of information provided to the State Commissioner for Data Protection and Freedom of Information must be provided. The sentences 4 to 6 rules the procedure of exchange of information and the dissemination of the results of the test on the data subjects.

The format of the information referred to in paragraph 7 is a matter for the discretion of the authority. The information can also be issued by provision of copies or

inspection. The interest of the person concerned is to be taken into account when exercising its discretion.

Paragraph 8 is used for the implementation of Article 15 paragraph 4 of Directive 2016/680 (EU).

On Article 55 **File inspection rights**

Article 55 uses Article 41 of JVollzDSG SH in the previous version.

The first sentence of paragraph 1 of Article 14 of Directive (EU) regulates 2016/680 going beyond the requirements of the act no view to the right of the data subjects. Sentence 2 makes clear that the file with a lock, duly stamped components, is not subject to the inspection.

The first sentence of paragraph 2 determines which people in one inspection of delivery can be consulted. Sentence 2 shall authorize the sole inspection by the ombudsman. The prisoners are to avoid dependencies and subcultural behaviour in prison, sentence 3 sets out that the involvement or commission of inmates is not permitted.

Paragraph 3 grants the data subject the right to take notes from the file.

Paragraph 4 lays down the conditions under which the data subjects are to leave photocopies or printouts of individual documents.

Paragraph 5, sentence 1 normalizes the gratuitousness of the inspection. Sentences 2 and 3 rules the obligation to reimburse the cost of photocopies and prints and the advance payment obligation. This is in accordance with the provisions of Article 12 paragraph 4 of Directive (EU) 2016/680, to the effect that the administrative costs for the provision of information, taking into account the payment of an appropriate fee can be paid. According to sentence 4, law enforcement, in exceptional cases, as in the case of correspondence and telephone calls as a consequence of the social state principle the costs incurred for the prisoners to a reasonable extent, if these are not in a position to do so.

On Article 56 **Information and inspection of files in health records**

In the implementation of the decision of the Federal Constitutional Court from December 20, 2016 (2 BvR 1541/15) section 56 sentence 1 the prisoners have the right of information regarding their health and access to their health records. By the referral in sentence 2, among other things, the involvement and engagement of certain persons and the cost arrangements for the inspection of section 55 shall apply mutatis mutandis.

On Article 57 **Lock flags**

Article 57 essentially corresponds to Article 42 paragraph 1 and 2 of JVollzDSG SH in the previous version.

Paragraph 1 provides for securing the right to inspection of an exhaustive list of the reasons for fitting a lock mark. The determination relates only to the inspection of law pursuant to Article 55; this is not covered by Directive (EU) 2016/680. In accordance with Article 55, paragraph 1, sentence 2 shall be subject to the act components, with a lock note, not the inspection; this does not affect the general right to information according to Article 54. The provision of administrative simplification enables directly during the recording of a document in the file the taking of a decision on a later disclosure.

The information interests of the prisoners must be withdrawn if medical reasons alone for the good of the prisoners, the protection of the above-mentioned legal goods or a common law duty of confidentiality claim priority. Sentence 1 requires a good balance in individual cases, in accordance with the scope of paragraph 2 on the basis and extent should be documented. Number 1 is to be interpreted strictly, in order to avoid informational paternalism. However, in certain special cases, for example in connection with psychiatric treatments, a lock mark in favour of the data subjects may also be justified.

Limiting the circle of persons authorized to apply lock marks under sentence 2 ensures restrictive and professional handling.

On Article 58 **Procedures for the exercise of the rights of the data subjects**

The provision is based on the requirements of Article 12 of Directive (EU) 2016/680.

Paragraphs 1 and 2 transpose the provisions of Article 12 (1) to (3) of Directive (EU) 2016/680 on communications and modalities of communications to prisoners and other data subjects.

Paragraph 3 makes use of the possibility provided for in Article 12 paragraph 4 of Directive (EU) 2016/680, to refrain from a decision of the applicant or a more detailed justification in the case of a manifestly unfounded or excessive application. As an example, the frequent non-repetitive repetition of applications is mentioned as a possible reason for refusal to provide information.

Paragraph 4 is used for the implementation of Article 12 paragraph 5 of Directive 2016/680 (EU).

Section 9

Deletion, limitation of processing and correction

On Article 59 **Deletion**

Paragraph 1 sentence 1 largely corresponds to Article 43 paragraph 1 sentence 1 of JVollzDSG SH in the previous version. Paragraph 1 sentence 2 builds on Article 43 paragraph 1 sentence 3 of JVollzDSG SH in the previous version and with Article 43 paragraph 3 sentence 4 is essentially in JVollzDSG SH in the previous version.

Paragraph 1 normalizes the principle of mandatory deletion of personal data, unless one of the exceptions listed there applies. The exceptional case where the personal data is still required in order to achieve completion of purposes, for example, can be fulfilled where prisoners on parole or supervision will be dismissed. Paragraph 1 is thus also the implementation of Article 4 paragraph 1 point e of Directive (EU) 2016/680.

The first sentence of paragraph 2 obliges the law enforcement authorities to review annually whether personal data should be deleted. Sentence 2 regulates the annual period. In other cases, personal data from unauthorized persons such as prison visitors can be entered. Paragraph 2 is thus also the implementation of Article 5 of Directive (EU) 2016/680 (see also recital 26 at the end).

In paragraph 3, sentence 1, in each case for the enforcement of the penalty of imprisonment, juvenile detention, juvenile custody and other deprivation of freedom has normalized individual deletion periods. The standard contributes to Article 6 of Directive (EU) 2016/680, as far as possible between the personal data of different categories of people who will be affected, a distinction has to be made. Sentence 2 determines the exception to sentence 1 for cases in which a special provision, such as the judicial retention regulation of a region, requires a longer retention period for the prisoner's personal files. In these cases, there is a limitation of the processing in accordance with Article 60, paragraph 1, point 7.

Paragraph 4 also takes account of the distinction in custody types, as provided for in article 6 of Directive (EU) 2016/680 and follows from the legal presumption of innocence. Under this rule, not only the personal data of these prisoners, but also

that of their relatives and visitors, will be concerned. A further processing of this personal data is no longer needed after the dismissal of the prisoners.

On Article 60 **Limitation of processing**

Paragraph 1, point 3, 4, 6 and 7 basically correspond to Article 43 paragraph 5 points 2-5 of JVollzDSG SH in the previous version. Paragraph 3 is broadly in line with Article 43 paragraph 8 in the previous version and JVollzDSG SH (4), in turn, in essence, with Article 43 paragraph 9 of the JVollzDSG SH in the previous version.

In paragraph 1, Sentence 1, Article 16 paragraph 3 of Directive 2016/680 (EU), instead of the deletion of personal data for certain reasons, a limitation of its processing is possible.

Number 1 concerns high-level interests of risk prevention, security and law enforcement, recognized by Directive (EU) 2016/680 as processing purposes.

Number 2 ensures that interests of the regions and people who will be affected after the dismissal claimed and can be enforced. For example, prisoners have worked in law enforcement, even several years after their dismissal of the proof of these occupations compared to other public bodies may be required. A case in point 2 can also exist where the assertion of official liability or compensation claims is included. If there is evidence from the prisoner's personal file that a fact has to be proven at a later stage, a restriction of its processing is possible instead of the deletion of the personal data.

Number 3 sets the thoughts from number 2, after the deletion of the enforcement of rights of the data subjects must not interfere with or thwart (see recital 47 of Directive (EU) 2016/680).

In order to enable data subjects to exercise their rights and to effectively control data processing, paragraph 4 provides for a further limitation.

Number 5, the derogation provided for in Article 16 paragraph 3 point b of Directive (EU) in order to understand and thus far, the 2016/680 is also known in relation to numbers 1 to 4.

Number 6 contributes to, among other things, the technical conditions standing in the way of a deletion.

Number 7 provides for different statutory retention periods with an appropriate exception to the deletion.

In paragraph 1, sentence 2 obliged the documentation of the reasons for the restriction of the processing of personal data.

Because of the exceptional nature of the restriction to the processing of personal data, the processing of this data only under the conditions referred to in paragraph 2, sentence 1 is possible and admissible. If the processing of such data for the purposes to which their deletion is omitted, no longer required, this data shall be deleted immediately. The scheme is based on the principle of proportionality requirement of Directive 2016/680 (EU) and section 32, paragraph 2, sentence 3 of the Federal criminal law.

The second sentence of paragraph 2 of Article 5, Sentence 2 picks up the thoughts of Directive (EU) 2016/680 on procedural steps to ensure that deadlines are met.

Paragraph 3 provides, in addition to the consent of the data subjects in number 1, as set out in section 2 of the most important application for cancellation of the restriction to the processing of personal data in the event of a renewed detention. In this case, the law enforcement authorities may access the personal data to the former law enforcement authorities' behaviour or treatment measures. The law enforcement authorities will be able to return to the previous enforcement measures without any loss of information of the prisoners. The recourse to the already existing data for the prisoners is regularly less stressful than their new elevation. If the restriction of the processing of personal data is cancelled again, the deletion of this data again takes place in accordance with Article 59.

Paragraph 4 sentence 1 makes it clear that, even in cases in which the processing of personal data is limited, the maximum limits for the retention must not be exceeded and sets out in sentence 3, the period shall begin. Sentence 2 is nevertheless an exception to the maximum limits for the retention, if a case referred to in paragraph 1, so concrete indications that the personal information to law enforcement or to remedy a proof snot are required.

On Article 61 **Rectification**

The arrangements referred to in paragraph 1, Sentence 1, contains an implementation of the principle from Article 4 paragraph 1 point a and d in conjunction with Article 7 paragraph 2 of Directive (EU) 2016/680 that personal data is corrected if it is inaccurate, incomplete or out-of-date.

In paragraph 1, sentence 2 takes over the in recital 47 of Directive (EU) 2016/680 for the ideas contained. To prevent major and unsuccessful applications in the prisons, it is necessary to clarify that the right of the person concerned about facts and not on the content of statements of witnesses, assessments or decisions.

In paragraph 1, sentence 3, article 4 paragraph 1 point d 1. Half-sentence, Directive (EU) 2016/680.

Paragraph 1 sentence 4 takes over Article 20, paragraph 1, sentence 2 of the German Federal Data Protection Law in the version promulgated on January 14, 2003 (BGBl. I p. 66), the last by Article 10 paragraph 2 of the law of October 31, 2017 (BGBl. I p. 3618) has been changed and substantiates this.

In accordance with paragraph 1, sentence 5, Article 16, paragraph 1, sentence 2 of Directive (EU) 2016/680 implements that the data subject is to complete their incomplete personal data by a supplementary declaration. This should act to preserve the clarity and truth and also act for other adjustments.

Paragraph 2 regulates a further case of the restriction of processing. Article 16 paragraph 3 point a of Directive (EU) 2016/680 includes the (legitimate) correction of incorrect data deletion as a subcase. In accordance with Article 58, paragraph 1, sentence 3 and 4 of the German Federal Data Protection Act, as amended in its notice of June 30, 2017 the deletion due to correction of incorrect data in the justice data protection act systematically as a case of correction are detected (see also the explanatory memorandum to the bill of the Federal Government dated February 24, 2017, BT-printed matter 18/11325, page 114). The abolition of the restriction of the processing according to sentence 2 therefore leads either to correct the data or the full processing.

On Article 62 **Rights of the data subject to correction and deletion as well as limitation of the processing**

The rule is used for the implementation of Article 16 of Directive (EU) 2016/680 in so far as this affects rights. The implementation of the obligations contained in this article objective of law enforcement is in Articles 59 to 61.

Paragraph 1 is used for the implementation of Article 16 paragraph 1 of Directive 2016/680 (EU).
Sentence 1 in Article 16 paragraph 1 of Directive (EU) 2016/680 grants the right to correct inaccurate or incomplete data. The sentence 2 implements the second sentence of Article 16, paragraph 3.

Paragraph 2 sets out - in conjunction with Article 59 - the provisions of Article 16 paragraph 2 of Directive (EU) 2016/680.

Paragraph 3 is used for the implementation of the procedure provided for in Article 16 paragraph 4 of Directive (EU) 2016/680 and subject to the applicable procedures, if the person responsible fails to comply with an application for rectification or deletion or only to a limited extent.

On Article 63 **Notifications**

The obligation contained in this provision is Article 7 paragraph 3 and Article 16 paragraphs 5 and 6 of Directive (EU) 2016/680.

In paragraph 1, sentence 1 provides for the correction, deletion or restriction of the processing of personal data and other places to which this data was previously submitted to give note, so as to ensure the correctness of the data for further transmission operations.

In sentence 2 of the controlled undertaking of the recipient, the correction published in the data set follows immediately from the responsibility to correct any incorrect data.

Paragraph 2 is used for the implementation of Article 5, sentence 2 of Directive (EU) 2016/680.

Section 10

Application of other provisions and final provisions

On Article 64 **Application of the other requirements of the general data protection law**

As far as for data protection in law enforcement is concerned, unless otherwise specified in this act, this shall take place in accordance with paragraph 1, sentence 1 of the General Data Protection Law. Sentence 2 explains, in particular, that Articles 5 to 16, Articles 60, 61, 65, 66, 68, 69, Articles 78 to 81, Article 83 and Article 84 of the German Federal Data Protection Act shall apply accordingly because there are already regulations in place with sample function without region-specific characteristics.

Paragraph 2 contains, in purely declaratory terms, the statement that for the processing of personal data by law enforcement authorities in the material scope, Regulation (EU) 2016/679 shall apply exclusively with its provisions and the provisions adopted for this purpose. This is the case if, for example, the data processing from the outset is not within the scope of Article 1, paragraph 1 of Directive 2016/680 (EU), for example, because it involves the management of employee data. Furthermore, Regulation (EU) 2016/679 may apply because personal data that is collected for the purposes of law enforcement is also processed for purposes other than those specified in EU Directive (2016/680). In these cases, Regulation (EU) 2016/679, as laid down in Article 9 paragraph 2 of Directive 2016/680 (EU), unless the processing is carried out within the framework of an activity, which is not in the scope of Union law.

On Article 65 **Entry into force, Termination**

Paragraph 1 governs the entry into force of this law as well as the expiry of the relevant data protection legal provisions in the enforcement laws of the regions.

Paragraph 2 establishes a transitional regime for the reporting requirements for automated processing systems required by Article 25, Paragraph 1 of Directive (EU) 2016/680, thus making use of the corresponding authorization in Article 63 (2) of Directive (EU) 2016/680 (recital 96) which, in exceptional cases where the conversion of the automated processing systems is already established before the Directive entries into force, involves a disproportionate effort, as in the case of BASIS-Web, allows a postponement of the entry into force until May 6, 2023.