1 National priorities

1.1 Putting the finishing touches to the European data protection reform and JHA Directive

After almost four years of protracted negotiations, in December 2015 the Council of the European Union and the European Commission agreed on wording for the General Data Protection Regulation and the directive for data protection in the police and justice sector.

In my last two activity reports, I have already discussed the European Commission's reform proposals and the progress of negotiations in great detail (see 24th activity report, no. 2.1; 25th activity report, no. 1).

In 2015, the negotiations were finally completed. After the European Parliament had agreed on its proposals in March 2015, the EU's Justice and Home Affairs Ministers adopted a joint position on the General Data Protection Regulation (GDPR) in June 2015.[1] In October 2015, agreement was reached also on the proposal for a Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (JHA Directive).[2]

During the subsequent informal trilogue, representatives of the Council, the European Parliament and the European Commission negotiated intensively to reach agreement on both legal acts before the end of 2015. Together with my counterparts in the EU and in Germany, I contributed to the discussion by putting forward constructive proposals. In their individual – but very similar – position papers, both the Article 29 Working Party[3] and the Conference of Federal and State Data

---

1 Cf. Council document 9565/15, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
2 Cf. Council document 12555/2015, http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/en/pdf
3 Paper of 17 June 2015 "Core issues in the view of trilogue", http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf; and on JHA Directive WP 233

Protection Commissioners[4] addressed important and critical issues to be taken into account during the trilogue on both legal acts. Together with some state commissioners for data protection, I had the opportunity to present the positions of German data protection authorities to the European Parliament, the Council Presidency and the European Commission.

In December 2015, the trilogue parties agreed on the final wording for both legal acts. After the necessary editing and translation, the Council and the Parliament adopted the legal acts in April 2016. They were published in the Official Journal of the European Union on 4 May 2016. The GDPR entered into force on 25 May 2016, the JHA Directive on 5 May 2016. **The GDPR will be applicable in all member states from 25 May 2018, and the JHA Directive must be implemented in national law by 6 May 2018.**

In my view, the conclusion of the European data protection reform sends a positive signal. The global and ubiquitous processing of personal data, the rapid emergence of ever new business models and Big Data applications as well as government surveillance require a global response. In this respect, the new European legislation is essential.

First of all, it is a huge success that such an agreement could be reached at all. Given the many very different interests of citizens, businesses, the research community and government institutions, it is no small accomplishment that all 28 member states and the European Parliament have agreed on a common legal framework for the coming years. This holds true in particular for the JHA Directive which – for the first time ever – creates a uniform EU-wide minimum standard also for national processing of personal data in the area of police and justice.

The new data protection legislation is very important for people and businesses in Europe. In particular the private sector will be subject to a largely uniform European data protection legislation which will be enforced in a uniform way in all matters

---

[4] Core issues for the trilogue negotiations on the General Data Protection Regulation, https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/20150826_Verbesserung%20DSGrundverordnung.pdf?__blob=publicationFile&v=3 (in German); Core issues for the trilogue negotiations on the Data Protection Directive in the area of justice and home affairs, https://www.bfdi.bund.de/SharedDocs/EU/ModernisierungDSRecht/DSK_Kernpunkte_Trilog_de.pdf?__blob=publicationFile&v=1 (in German)

relevant across Europe. This will make it easier for Europeans to exercise their rights and create a level playing field for businesses in the European market. Due to the marketplace principle (cf. 24th activity report, no. 2.1.1), the impact of European data protection legislation extends well beyond Europe. Non-European companies, too, will have to abide by EU rules if they want to do business here.
During the trilogue negotiations, the Council draft was significantly improved, including and implementing several key requests of national and European data protection commissioners:

For example, data minimization has been enshrined as an important principle in the GDPR. This is important in particular because in public debate some repeatedly argue that data minimization was obsolete and outdated in times of Big Data. However, the opposite is true: Big Data technologies make the dangers and threats described by the Federal Constitutional Court in its 1983 census decision become reality. Therefore, it is more important than ever to remember that linking data to create and analyse profiles always affects an individual's right of self-determination so that such interventions should be reduced to a minimum. The GDPR respects this approach based on fundamental rights, which I am very pleased about.

In addition, the limitation to specific purposes has been significantly strengthened as compared to the Council's proposals: Also in the future, data processing for purposes that are not compatible with the original purpose of collection will be allowed only with the data subject's consent or to meet important public interests. I will keep a watchful eye on this to ensure that this principle is not undermined by national laws (cf. no. 1.2.f).

Another positive aspect to be mentioned is that European regulators stood up for clear international rules on data transmission to authorities and courts in countries outside the EU.

From the perspective of German data protection law, we are delighted that a German success story is becoming European: In the future, all authorities – and in some cases of risky data processing also businesses – across Europe must appoint a data protection officer. Moreover, member states may provide for a mandatory

appointment of corporate data protection officers in additional cases. I expect that federal law-makers will use their discretion so that the two-pillar model consisting of corporate self-monitoring and government supervision can continue unchanged.

However, the new European legislation does not fulfil all wishes of data protection supervisory authorities. For example, some areas have been excluded from the necessary modernization of data protection legislation.

To strengthen self-determination in the digital age, consent must be designed such that the will of individuals can be clearly identified and that they have a true choice. Unfortunately, explicit consent will not be required in the future either. This gives global businesses in particular extensive possibilities for data processing by using standard data protection statements. Moreover, due to insufficient rules on profiling – one of the most important issues of data protection law – this practice will continue to be used very extensively.

I appeal to federal and state regulators to embrace the spirit and letter of the new European rules when amending national data protection law (cf. no. 1.2.f).

Please also refer to my brochure “Info 6” on the GDPR. In addition to the text of the regulation, the brochure gives an introduction to the General Data Protection Regulation.

1.2 Implementing the European data protection reform in national law

Germany’s data protection law must be aligned with the General Data Protection Regulation by 25 May 2018 (cf. no. 1.2.1). The directive governing data protection in the area of police and justice must be implemented even earlier – by 6 May 2018 (cf. no. 1.2.2). For both legal acts, the Federal Ministry of the Interior prepared a ministerial bill amending national data protection law and implementing EU legislation (*Datenschutz-Anpassungs- und Umsetzungsgesetz EU*, DSAnpUG-EU). Discussions on the bill within the Federal Government were still ongoing at the time of going to press.

Adoption of the amending legislation by the German Bundestag is planned in the 18th legislative term to ensure that it enters into force by 25 May 2018. The bill will in particular include the necessary amendments of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG). Ensuing amendments necessary in specific sectors will be subject to a separate legislative process. The DSAnpUG-EU requires Bundesrat approval.

1.2.1 Adapting national data protection law to the General Data Protection Regulation

The General Data Protection Regulation is directly applicable and binding in its entirety in all member states. Its aim is to create an equivalent level of protection of the rights and freedoms of natural persons with regard to the processing of data (recital 10). While the Regulation leaves some areas to the discretion of national regulators, it also requires member states to take specific legislative measures.

During negotiations on the national amending legislation, I asked that the Regulation's aim of harmonization be taken seriously and – where there is room for discretion – that provisions be adopted which ensure a high level of data protection. To give some examples:

National regulators should refrain from adopting provisions allowing data processing for other uses. Not only is the principle of purpose limitation essential from a German perspective, it is also enshrined in Article 8 of the EU Charter of Fundamental Rights and Article 5 (1)(b) of the GDPR.

According to Article 23 of the GDPR, the rights of data subjects granted by the Regulation (e.g. right to demand information, right to object) may be restricted only if this is proportionate and necessary to safeguard certain important interests. In my view, the new Federal Data Protection Act should make very modest use of such restrictions and allow them only after a thorough examination of each individual case. Also the restrictions under the current Federal Data Protection Act may be maintained only if they fulfil the strict requirements of Article 23 of the GDPR.

Germany will continue to have different supervisory authorities for monitoring and advising on data protection matters. When there are several supervisory authorities in one member state, the Regulation requires domestic coordination of certain procedures and of representation in European bodies. For example, the Regulation requires member states to designate a “single contact point” (recital 119) and appoint a “joint representative” for the European Data Protection Board (Art. 68 (4)). I asked that these tasks be assigned to the Federal Commissioner for Data Protection and Freedom of Information to ensure consistent representation of German supervisory authorities in Europe. The interests of the federal states must be appropriately taken into account because their data protection supervisory authorities are responsible for monitoring data protection in the private sector. Moreover, the DSAnpUG-EU must include clear and unambiguous provisions on communication and decision-making between the various supervisory authorities in Germany so that together, Germany’s supervisory authorities have a strong position in Europe.

1.2.2 Implementing the JHA Directive – Minimum harmonization does not equal standardization

The Data Protection Directive for the area of police and justice (JHA Directive) is the second pillar of the EU’s new data protection package and obliges member states to implement its provisions in national law by 6 May 2018.

The JHA Directive aims at minimum harmonization within the EU – a first for data protection in the area of police and justice. This is a most welcome intention. Minimum harmonization means ensuring a high level of protection across the EU. However, member states which already have a higher level of data protection should in no case adjust that level downward. The Regulation underlines this in its recitals. Member states should precisely not be precluded from providing higher safeguards than those established in the JHA Directive for the protection of the rights and freedoms of their citizens.

For implementation in Germany, this means the following: Where the JHA Directive makes stricter provisions than national law, national law must be amended

accordingly, and where national law is stricter, it should be maintained without exception.

Even during negotiations at European level, the scope of the JHA Directive in relation to the GDPR was widely discussed. Ultimately, the Directive does not conclusively specify whether and which other threat prevention authorities – in addition to police authorities – should fall under its scope during which activities. To avoid ambiguities, I recommend that the parliament adopts matching rules for all these authorities.

I would even go one step further: Although as part of national security, the activities of intelligence services are covered by neither the Directive nor the General Data Protection Regulation, I think that the same requirements should apply to them.

For my own activities and for the activities of other supervisory authorities, the future powers of data protection supervision will be crucial. In this respect, the Directive requires enhanced possibilities. Supervisory authorities must be able to effectively respond to violations, e.g. by issuing orders or imposing prohibitions. In addition, they must be given the power to initiate court reviews. Therefore, I recommend that the powers to initiate investigations, issue orders and take legal action under national law should be the same as in the GDPR.

Moreover, I consider the following provisions particularly important:

- Data subjects must have the right to be informed of the fact that none of their personal data have been recorded.

- Data processors must be obliged to establish a data protection management scheme to achieve data minimization, availability, integrity, confidentiality, non-linkability, transparency and intervenability.

- Controllers must be obliged to keep a record of all processing activities, preferably with the government data protection officer.

- Sector-specific requirements must be maintained on the basis of which administrative regulations (e.g. opening orders) specify the purpose, the legal basis, the group of data subjects, the type of data to be stored, the entry of data, requirements of data transmission, retention periods and necessary technical and organizational measures. The same applies to prior consultation of data protection supervisors when starting new databases or processing activities.

- In addition to recording user access, recording administrative access should be mandatory as well.

- When transmitting data to third countries, the Federal Constitutional Court decision of 20 April 2016 (1 BvR 966/09, nos. 329 - 341) on the Federal Criminal Police Office Act should be taken into account, unless EU legislation provides otherwise. According to the decision, the transfer of data to third countries presupposes a restriction to sufficiently weighty purposes for which the data may be transferred and used, the ascertainment that the data will be handled in the third country in acceptable conformity with the rule of law, the guarantee of effective domestic oversight, and specific and clear foundations in German law. In my view, effective and independent supervision requires an obligation of the transmitting bodies to record transmissions to third countries in a central place (cf. no. 1.3).

I will accompany the implementation of the JHA Directive at federal level and the future enforcement of implementing legislation from a data protection perspective.

1.3 Far-reaching decisions in the field of security

The Federal Constitutional Court reaffirms its previous rulings and imposes further requirements on the activities of the police and intelligence services. This has far-reaching consequences also for regulators and data protection supervision. Efficient supervision is of utmost importance also when German bodies transmit data to foreign security authorities.

A. Requirements of the Federal Constitutional Court

On 20 April 2016, the Federal Constitutional Court made another fundamental decision. The court decided on the Federal Criminal Police Office Act (*Gesetz über das Bundeskriminalamt*, BKAG), namely the newly added counter-terrorism powers. The requirements imposed by the court apply not only to the police forces, but also to intelligence services. The decision is in line with and builds on the court's previous decisions in the area of security.

According to the Federal Constitutional Court, **supervision of intelligence services is particularly relevant** (court order of 13 October 2016). Given the clandestine nature of infringements of fundamental rights in this area, the supervisory bodies' constitutional **compensating function** to protect the data subjects' fundamental rights is especially important.

Intensified **international cooperation** between security authorities and the ongoing – also technical – development of the European and international security architecture increase the importance of this compensating role and thus the tasks to be performed by the supervisory bodies.

The Federal Constitutional Court has repeatedly obliged regulators to grant supervisory authorities the personnel and material resources necessary to fulfil this compensating function. In this respect, there are still major deficits.

I. Efficient data protection supervision

As in its decision on the Act on Setting up a Counter-Terrorism Database (*Antiterrordateigesetz*, ATDG) of 24 April 2013, in its decision on the BKAG the court once again stresses the importance of external supervision to ensure that security legislation is in line with the Constitution. It also once again obliges regulators to ensure that supervisory authorities, including my authority, are able to fulfil their obligation to carry out efficient and effective controls, as required by constitutional court rulings (cf. Box b on no. 1.3 B and no. 10.2.10).

1. Mandatory controls

For the counter-terrorism database and the right-wing extremism database (cf. 21st activity report, no. 5.1.1; 24th activity report, no. 7.2 and no. 7.3), the court expressly requires data protection controls to be carried out regularly, at least every two years. In addition to these databases, there are many other joint databases which also fall under the court's rulings. These requirements also significantly affect the scope and intensity of my controls in this area because both the extent and the frequency of controls must be increased. These court requirements for regular monitoring have already been implemented in national law for the counter-terrorism database and the right-wing extremism database. However, so far I do not have sufficient personnel resources.

Monitoring these joint databases requires special effort (cf. Box a on no. 1.3). It is not enough to merely look into both databases to be able to assess the lawfulness of stored data. Such assessment is possible only if I also check the source database(s) of those bodies which stored these data, i.e. I must check whether the data were collected and stored in line with the rules for the source database(s). To do this, I must also check the interaction of these source databases with other databases of these authorities, taking into account many other related legal requirements (cf. Box a on no. 1.3). To do so, I must also access log databases.

Last but not least, to assess the lawfulness of data storage, e.g. in the counter-terrorism database, I must also check – as required by the Federal Constitutional Court – whether and which other measures have been taken by the storing body or other authorities participating in the counter-terrorism database with regard to the data subjects. This is the only way for me to find out whether a data subject was subject to total surveillance – which the Federal Constitutional Court considers unconstitutional – or to additive infringements of fundamental rights by an authority or several authorities together. To put it in a nutshell: To be able to check a single entry, e.g. in the counter-terrorism database, in accordance with the requirements of the Federal Constitutional Court, checking further databases of other authorities is indispensable. This takes a long time and requires a huge logistical effort.

2. Monitoring data transmission to foreign security authorities

To protect the fundamental rights of data subjects, the Federal Constitutional Court requires efficient monitoring also when German security authorities transmit personal data to foreign security authorities. The court emphasizes that its requirements for such data transmission must be effectively and efficiently monitored and that transmissions are effective only with such monitoring. This means that **without effective monitoring**, these **transmissions are unlawful** and therefore not permitted.

The revelations of Edward Snowden and the research of the first committee of investigation of the German Bundestag in the 18th legislative term on the activities of security authorities of the so-called Five Eyes countries in the Federal Republic of Germany (cf. no. 10.3.6) brought international cooperation of intelligence services to the critical attention of the public. Given the flaws and violations which occurred in the course of such cooperation, it is especially important to rigorously monitor whether the transmission requirements of the court (cf. Box b on no. 1.3) are fulfilled.

3. Monitoring intelligence services – “Special relevance of supervision”

Intelligence services have special tasks and powers. They must take action long before specific threats arise, and they must recognize such threats to our liberal democracy as early as possible. Special tasks and powers enshrined in our national legislation allow them to do this. For this reason, intelligence services are allowed to extensively and secretly – and earlier than any other authority – infringe on data subjects’ fundamental rights. Due to this special status, it is inevitable that certain leads will bring innocent people to the attention of intelligence services. Therefore, in its order of 13 October 2016, the Federal Constitutional Court once again emphasized the “**special relevance of supervision**” and the “**special awareness-raising role**” of supervision in the field of intelligence services.

a) Compensating function of data protection supervision

Given this special status of intelligence services, special compensation is needed to protect the fundamental rights of data subjects (cf. Box b on no. 1.3 B). The Federal Constitutional Court assigned this task to the supervisory bodies, including my authority.

b) Additional technical and personnel resources for intelligence services; international cooperation

Given the rapid technical progress, intelligence services continue to add significant resources in terms of both technology and staff.
Terrorists and criminals increasingly and very skilfully use technical means, including mobile telecommunications and the Internet, in particular the so-called darknet. They also extensively use social networks and social media for their propaganda. Therefore, it is crucial for security authorities to keep up with these developments and to intensify cooperation at international level.

To be able to do this, the services need the right conditions and a constitutional legal framework. However, necessary legal amendments must comply with the Constitution and data protection law, in particular when it comes to the compensation required by the Federal Constitutional Court, i.e. the ability of independent supervisory bodies to effectively review these measures.

Regulators used various approaches to amend a series of laws, including the Act on the surveillance of communications between non-German citizens abroad by the Federal Intelligence Service (*Gesetz zur Ausland-Ausland-Fernmeldeaufklärung*) and the Act to improve information-sharing in the fight against international terrorism (*Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus*). In addition, they gave intelligence services far-reaching new powers, in particular as regards cooperation and information-sharing with foreign security authorities (cf. no. 10.2.10.1).
These new powers and technical capabilities heavily infringe upon citizens' fundamental rights. They are often very broad and carried out secretly, i.e. without

the knowledge of data subjects. To protect the data subjects' fundamental rights, it is therefore essential that independent supervisory bodies, including my authority, compensate for the limited possibilities of legal redress by carrying out **efficient and effective controls** (cf. no. 1.3 and no. 10.2.10.2).

II. Further requirements of the decision on the BKAG

The requirements of the Federal Constitutional Court "concern specific wide-ranging potential threats to fundamental rights, in particular those entailed in the context of electronic processing of data ..., as well as individual case-by-case measures against persons who are being focussed on by the acting authorities." This means that **all measures heavily infringing on the right to informational privacy** must comply with these standards. Infringements are proportionate only if effective data protection supervision is ensured.

Regulators must now align the legal basis for intrusive powers of security authorities and intelligence services to the Constitution, i.e. they must also amend existing provisions accordingly. The following requirements need to be kept in mind:

- Infringement thresholds and target groups

  For example, laws mention or simply imply the possibility to include contact and accompanying persons in surveillance. Many of these provisions are not in accordance with what the Federal Constitutional Court has in mind, unless they correspond to the provisions of Section 20b (2) no. 2 of the BKAG. In particular the laws on intelligence services limit the target group very insufficiently.

- Purpose limitation and transmission rules

  The court has fully outlined the constitutional requirements of purpose limitation when using personal data, including requirements for both the use of data within an authority and the transmission to other bodies.

  According to the court, personal data obtained during investigations which heavily infringe upon fundamental rights may be transmitted only if a balanced protection of legal interests is ensured. In addition, there must be sufficient specific evidence for further investigations. A merely potential informative value or even general

relevance are not sufficient. For this reason, **all provisions on the transmission of personal data** under security law must be fundamentally **revised**. For intelligence services, this derives from the decision on the counter-terrorism database and the principle of separation of information developed in this decision (cf. 25th activity report, no. 5.2).

- Transmissions abroad

  Special rules apply to **transmissions abroad**. In this respect, current provisions on the protection of the Constitution have major deficits. For example, Section 19 (3) of the Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution (*Bundesverfassungsschutzgesetz*, BVerfSchG) lack a provision corresponding to Section 14 (7), sixth, eighth and ninth sentence of the BKAG. This provision governs the notification of the recipient of when the data should be deleted, the consideration of a data subject's protectable interests in the individual case and the existence of an appropriate level of data protection in the receiving country. The transmission requirements under Section 14 (1), first sentence, nos. 1 and 3, second sentence, of the BKAG are not in line with the Constitution either. This applies to Section 19 (3) of the BVerfSchG accordingly.

- Procedural safeguards

  Provisions on court orders, transparency, logging and data protection supervision should also be revised across the entire security law.

  In particular in the area of secret data processing, the weak protection of individual rights must be compensated by efficient, effective and regularly scheduled data protection controls (see above). Police authorities increasingly operate secretly as well, although they are obliged to gather data openly. However, in its capacity as a central office, the Federal Criminal Police Office frequently processes data without data subjects being aware of it, much less expecting it. With the new police information networks which establish connections and compare data in the background it can be assumed that such covert data flows will increase in the future.

Moreover, the compensating function can be effective only if the authorities concerned respond to my objections in the same way as to decisions by administrative courts. However, I have **no authority to give instructions** to the offices for the protection of the Constitution. Nor does current legislation allow me to initiate court proceedings. As regards police authorities, this is not in line with the new EU directive on data protection in the area of justice and home affairs (JHA Directive, cf. no. 1.2.2).

B. Current laws/bills – non-compliance with requirements of the Federal Constitutional Court

Current acts and bills also have significant shortcomings with regard to compliance with constitutional court requirements.
One example is the draft Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (*Datenschutz-Anpassungs- und Umsetzungsgesetz EU*, - Bundestag printed document 18/11325 - cf. no. ...). The draft also amends the Federal Intelligence Service Act (*BND-Gesetz*, BNDG) (Art. 4, Section 32 and Section 32a (1) no. 1 (b) of the draft BNDG). However, these amendments do not reflect the Regulation. Contrary to applicable law and the aforementioned constitutional court requirements, they are instead intended to **restrict my powers**. I hope that regulators will follow my objections and refrain from enacting these provisions.

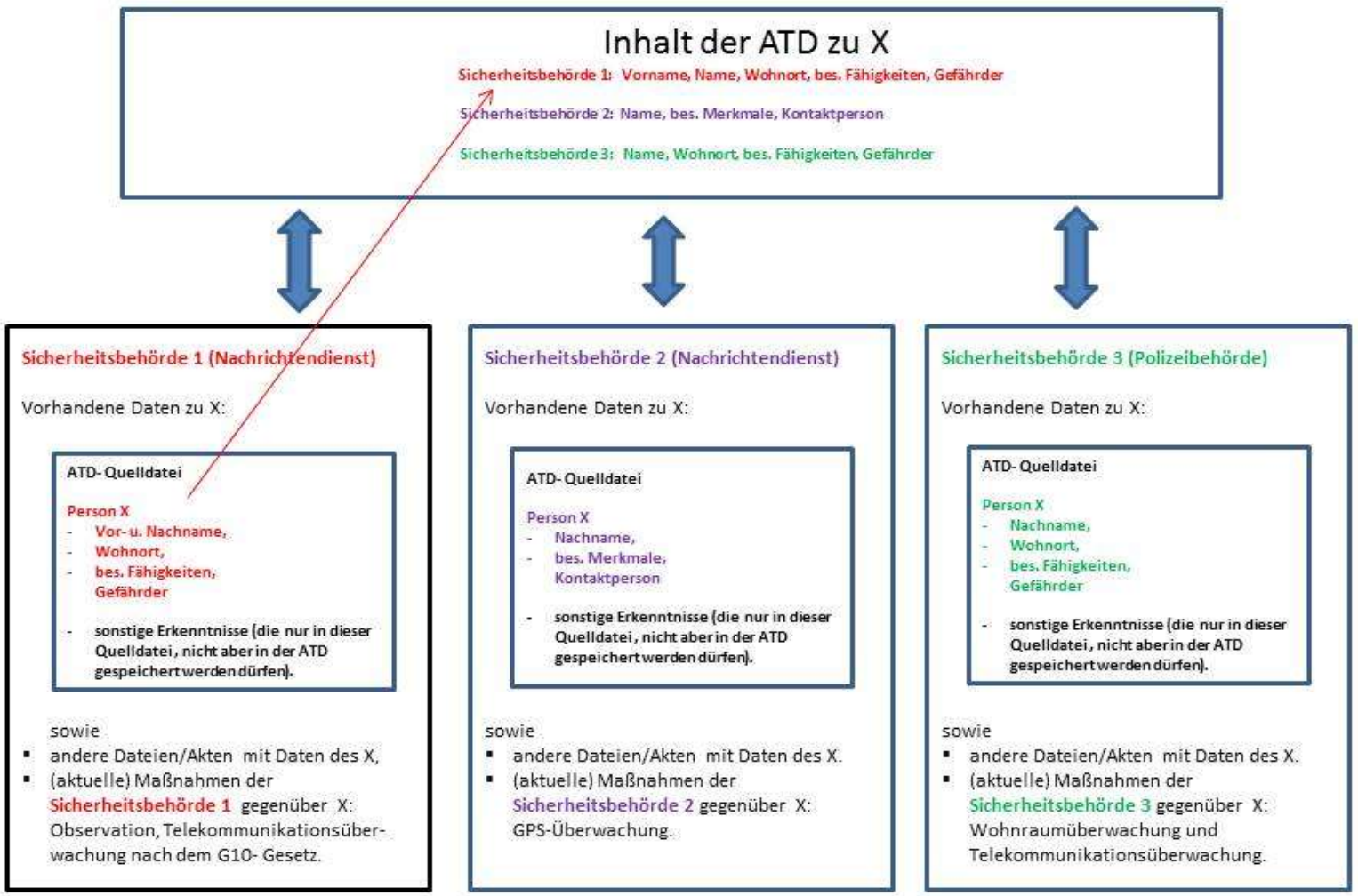
C. Budget implications

The Federal Constitutional Court ruled that appropriate provisions in the budget should be made to significantly increase staff at my agency in the coming fiscal years. Fortunately, initial steps have been taken in the reporting period. Without a continued increase in staff, the requirements of the Federal Constitutional Court cannot be fulfilled.

Box a on no. 1.3

Fiktives Beispiel: Kontrolle einer Person (X) in der ATD

- drei Sicherheitsbehörden des Bundes haben Daten zu X in der ATD gespeichert ; diese stammen aus den jeweiligen ATD-Quelldateien dieser Behörden -



Box b on no. 1.3

Erläuterungen zum fiktiven Beispiel: Kontrolle einer Person (X) in der ATD

- drei Sicherheitsbehörden des Bundes haben Daten zu X in der ATD gespeichert -EEE

(Verfassungs-)rechtlich vorgegebener Ablauf / Umfang der Kontrolle:

1. **Prüfung der ATD-Speicherung der Sicherheitsbehörde 1 wie folgt:**

   a) Ist die ATD-Speicherung nach den Vorgaben des ATDG zulässig.
   b) Sind die Daten aktuell und identisch in der (den) ATD-Quelldatei (en) gespeichert.
   c) Ist die Speicherung in der Quelldatei rechtlich zulässig (entspricht sie insbesondere den Vorgaben der einschlägigen Dateianordnung; falls nicht, ist die ATD-Speicherung unzulässig).
   d) Wurden die in der Quelldatei gespeicherten Daten rechtlich zulässig erhoben (falls nicht, ist die ATD-Speicherung unzulässig).
   e) Liegen verfassungsrechtlich unzulässige „additive Grundrechtseingriffe" zu Lasten des X durch diese Sicherheitsbehörde vor, d.h. Ermittlung und Bewertung aller bei dieser Sicherheitsbehörde zu X vorhandenen Daten / Maßnahmen (Vorgabe des Bundesverfassungsgerichts).

2. **Prüfung der ATD-Speicherung der Sicherheitsbehörde 2 wie folgt:**
   Siehe oben 1 a) – e).

3. **Prüfung der ATD-Speicherung der Sicherheitsbehörde 3 wie folgt:**
   Siehe oben 1 a) – e).

4. **Prüfung aller Daten/Maßnahmen aller Sicherheitsbehörden**
   Liegen unzulässige „additive Grundrechtseingriffe" zu Lasten des X durch das Zusammenwirken der Maßnahmen aller Behörden vor.
   Notwendig ist demnach eine Zusammenschau und Bewertung der zu X bei allen Behörden vorhandenen Daten / Maßnahmen (Vorgabe des Bundesverfassungsgerichts). Konsequenz: Eine bzw. einzelne Maßnahmen könnten - rechtlich isoliert betrachtet - verfassungsrechtlich zulässig sein und sich erst in dieser Zusammenschau als verfassungswidrig erweisen. Die Sicherheitsbehörden sind verpflichtet, dies durch eine entsprechende Kooperation / Abstimmung auszuschließen (Vorgabe des Bundesverfassungsgerichts).

Key requirements in recent decisions of the Federal Constitutional Court:

A. Transmission of personal data to foreign security authorities (cf. decision on the BKAG)

- The police and intelligence services are bound to uphold fundamental rights. **The limits of domestic data collection and processing set by the Basic Law must not be undermined** by an exchange.
  "Under no circumstances may the state be complicit in violations of human dignity."

  According to the court, data may be transmitted only if

  - it can be expected that **in the receiving country, the data will be handled in sufficient conformity with rule-of-law standards, i.e. in line with data protection law and commensurate with fundamental human rights safeguards**, and

  - **effective supervision by the responsible German supervisory bodies is ensured**.

- The purpose of transmission and use must meet the **"criterion of a hypothetical new collection of data"**.
  "Thus, the transfer must pursue the aim of detecting criminal offences or protecting legal interests comparable in weight to those for which data were originally collected."

- A **"generalizing factual assessment regarding the legal and factual situation"** in the receiving country is sufficient proof of whether the required protection level, i.e. an appropriate material data protection level, is guaranteed in the receiving country only as long as it is not opposed by facts to the contrary. In this case or if the German body cannot make such an assessment, **"it is necessary to conduct a fact-based case-by-case assessment that determines whether it is at least guaranteed that essential requirements for**

the handling of data are sufficiently met". This assessment must be **based on substantial and realistic information** and **updated regularly**. The reasons must be **documented in a comprehensible manner**. If necessary, binding assurances or binding individual guarantees can and must be provided by the foreign body or the receiving country. However, data must not be transmitted if it is to be expected that the assurance will not be adhered to in the individual case.

"Further requirements are that the Federal Data Protection Commissioner has the opportunity to review the decision and that it may be subject to judicial review."

B. Effective supervisory control (fulfilling the supervisory bodies' compensating function) – case law (cf. decision on the BKAG):

Referring to its previous decisions, the Federal Constitutional Court once again stressed the importance of effective supervisory control, i.e. the compensating function of supervision to protect the fundamental rights of data subjects. This is a key prerequisite for effective administrative measures. The court once again obliges regulators to ensure this. This means that the supervisory bodies must be given appropriate resources so that they can fulfil their compensating function. The following statements of the court are particularly important:

"Since with regard to covert surveillance measures, the transparency of data collection and data processing as well as the facilitation of the protection of the rights of individuals can be ensured only to a very limited degree, the **guarantee of effective supervisory control is all the more significant**.

"With regard to surveillance measures that constitute serious interference with privacy, the principle of proportionality therefore places **more rigorous demands on the effective design of this supervision** both at the **level of the law** itself and in **administrative practice**.

"To begin with, the guarantee of effective supervisory control requires a body vested with **effective powers**, such as, under current law, the Federal Data Protection Commissioner. Since **supervisory control has the function of compensating** for weak protection of the rights of the individual, it is particularly

important that it be **carried out regularly**. This must be taken into account with regard to the funding of the supervisory body. **Guaranteeing compliance with the constitutional requirements for effective supervisory control is the joint responsibility of the legislature and the authorities."**

1.4 The connected and automated vehicle – not without data protection

The privacy implications of digital solutions for motor vehicles are gaining increasing attention.

During the reporting period, not only experts but also the media had long and controversial discussions about data protection in motor vehicles. "Cars as computers on wheels" and "cars as data-consuming monsters" have become buzzwords in these discussions. Since the Federal Government's Smart Networks Strategy put a greater focus on automated and connected driving, it has become even more important.

The car in particular is a symbol of personal freedom and independent mobility. The automation and networking of vehicles more or less counteracts this effect. Automated and connected cars are expected to improve traffic safety and driving comfort. However, the individual rights and freedoms of owners, drivers and passengers must not fall by the wayside. Regulation and the freedom to conduct a business must end where they inadmissibly restrict individual rights.

In the conference of independent federal and state data protection authorities, my counterparts in the federal states and I repeatedly addressed the use of vehicle data in a privacy-friendly way. We identified the following key points:

- All data generated by operating vehicles are influenced by the individual use of the vehicle and therefore personal. This means that there are no data which per se are not relevant under data protection law.

- The automotive industry is responsible for designing its products in compliance with data protection law and to encourage suppliers and providers of ancillary services that use the car's technical infrastructure to do the same.

- Therefore, the automotive industry is also obliged to comply with the data protection principles of Privacy by Design and Privacy by Default.

- Vehicle users must have maximum transparency regarding the data collection and processing operations in the vehicle.
- Suitable state-of-the-art technical and organizational measures must ensure data security and data integrity. This applies in particular to data communication from the vehicle.

Dialogue with the German Association of the Automotive Industry

In December 2014, the federal and state data protection authorities entered into a dialogue with the German Association of the Automotive Industry (VDA). A first positive result was achieved in early 2016, when they adopted a joint declaration on data protection aspects when using connected and non-connected vehicles (cf. Annex 3). In this declaration, the manufacturers and suppliers represented by the VDA commit themselves to the data protection principles. In particular, they recognize that vehicle data are personal data, at least when they are linked to the vehicle identification number or the vehicle's number plate. The touchstone for this commitment will be how manufacturers and suppliers fulfil their transparency obligations under data protection law and whether vehicle data will be collected and processed only with the owner's and possibly the driver's and passenger's consent. Vehicle users must continue to have full control over the vehicle data which may be used to analyse their driving behaviour. In the course of the dialogue, I will do my best to achieve this.

Round table on automated and connected driving

With the digital transformation in the automotive and transport sector, cyber security and data protection are becoming important issues also in this area. For example, I

advise the round table on automated and connected driving set up by the Federal Ministry of Transport and Digital Infrastructure, which brings together industry, academia, insurance and consumer protection representatives. They discuss solutions for issues arising from technical developments to promote automated and connected driving systems. It is already apparent that these systems will entail collecting and processing a yet unclear number of personal data. The necessary legal and technological safeguards must be thought through at an early stage to ensure that the data protection principle of Privacy by Design can be implemented. In the field of energy, the Federal Government has adopted the Act on the Digitization of the Energy Transition (*Gesetz zur Digitalisierung der Energiewende*), setting standards also for the automotive and transport sector (cf. no. 17.2.1). One example is the mandatory use of security certificates for communication components to improve the state of technology and thus protection from cyber attacks and uncontrolled data leaks. Connected vehicles, too, should communicate with other vehicles, the manufacturers' backend systems or third parties only via components that fulfil the minimum requirements for cyber security and data protection as specified in the technical guidelines for the Smart Meter Gateways used by the energy sector.

Car-to-car communications

In this context, I also deal with car-to-car communications. This technology allows vehicles to exchange driving and environment data via special wireless connections, e.g. to warn other drivers of dangers on the road or to autonomously avoid collisions at intersections. The information I have seen makes me increasingly concerned that the principle of data reduction and data economy is not sufficiently taken into account by those who develop the communication standards and specify the type and scope of data categories to be transmitted. In particular, insufficient precautions seem to be taken against tracking vehicles in the car-to-car network and identifying individual movement profiles on the basis of the driving data exchanged. Data protection and data security considerations are inseparable from each other also for this form of online communication between vehicles. Since the security of the transport infrastructure is of paramount importance, potential threats must be analysed and technical precautions must be taken on this basis. I will continue to monitor the

developments in this area and demand sufficient data protection and data security standards.

Outlook

I am well aware of the positive effects of technological progress in automotive engineering. Our society relies on mobility and will benefit from new systems which increase traffic safety, for example. However, these systems need many data that are generated when driving. Therefore, the industry must not neglect its responsibility for designing its systems in line with data protection law. Transparency, data minimization and giving data subjects as much control over their data as possible are important cornerstones.

Germany's automotive industry will gain a significant competitive edge if it seeks to maintain and expand its global market position by developing privacy-friendly products. Such technologies could not only be used in their own products but also be emulated by other manufacturers. I believe that customers will increasingly demand privacy-friendly technologies and take them as a measure of the trustworthiness of manufacturers.

1.5 Health apps and wearables – healthier with data protection

Health apps are becoming increasingly popular. Users are often not aware of the related privacy risks. The necessary transparency is lacking along with comprehensive and understandable data protection statements.

There is an ever-growing and dizzying array of health apps. Fitness, wellness, lifestyle, sport and "medical" apps are all health-related and, lacking a common definition, are collectively referred to as health apps, though few are medically relevant. What all of these apps have in common is that they electronically collect a large amount of the users' physical data. Only in very rare cases are these data stored exclusively on the device itself (e.g. smartphone, tablet, smartwatch, tracker). Usually, apps transmit these data to third parties. In many cases it is unclear where – in the country or abroad – these data are collected, processed and stored, by whom

and under which security conditions. Comprehensive and understandable data protection statements are missing. Users do not know what happens to their physical or health data, which are among the most sensitive personal data and require special protection. Health apps therefore pose significant privacy risks.

Moreover, poor technical data security often allows unauthorized parties to gain access to these sensitive data. Another significant risk for users is the unauthorized and uncontrolled linking and analysis of their data. Even if personal data from apps were anonymized, the physical data could be combined with the users' data freely available somewhere else so that re-identification would be possible. This way, businesses, insurance companies and others could create comprehensive health profiles of individuals and use them to the disadvantage of the unknowing users.

Many apps on various topics (e.g. nutrition, physical activity, stress management, vaccinations, health information, medical care, marketing, service) are offered by statutory and private health insurance funds. Statutory health insurance funds providing apps that collect health and thus social data have to observe the pertinent provisions of the Social Code specifying which social data may be collected and processed for which purpose. They are not allowed to process social data for other purposes, even if the data subjects have given their consent (unless in individual cases consent is provided for by law). Therefore, in each case they must examine whether the Social Code allows the collection of the data provided through apps. As a rule, this is not the case.

Private health insurance funds, however, may use apps in accordance with insurance contract law and general civil law. The use of apps must be agreed on in individual contracts. In this case, data protection is not governed by the Social Code but by the Insurance Contract Act (*Versicherungsvertragsgesetz*) and the Federal Data Protection Act. Nevertheless, the requirements of consent in accordance with data protection law and of the technical and organizational design of data collection, processing and use must be met. Ensuring transparency and informing users are particularly important. Regulators should consider granting the same level of protection to customers of private health insurance funds as granted under the Social Code to customers of statutory health insurance funds, i.e. allowing private health

insurance funds to collect health data via apps only if there is a specific legal basis for this.

In 2016 federal and state data protection supervisory authorities carried out random checks of devices and apps of different providers. They found that the manufacturers, operators and retailers of the reviewed devices and apps did not sufficiently inform users about what happens to their data. Most of the reviewed data protection statements did not fulfil the legal requirements, were too generic or were not even available in German. Many devices and the related user accounts did not allow users to delete all data themselves. Moreover, many devices and apps shared data with third parties without the users' knowledge, for example for research or marketing purposes. Many manufacturers only have service subsidiaries in Germany, while their main place of business is in other EU countries or even in third countries where European customer and data protection law does not apply. This will change only when the European General Data Protection Regulation enters into force in May 2018 (cf. no. 1.1).

In a resolution, the conference of federal and state data protection supervisory authorities called for effective protection of the sensitive health data of users of wearables and health apps (Annex 4).

Various initiatives to that effect have been launched at European level. In April 2014, the European Commission published a Green Paper on mobile health services. On this basis, the mHealth assessment guidelines working group composed of representatives of various public and private institutions from several member states developed criteria to assess the quality of health apps. The Code of Conduct on privacy for mHealth which introduces a system of voluntary commitment and is especially targeted at developers and producers of mobile applications was presented to the Article 29 Working Party in June 2016 for an assessment of its merits in terms of data protection. A subgroup of the Article 29 Working Party is currently discussing with the authors of the Code of Conduct to improve the level of data protection. Along with the review of the Code of Conduct on privacy for mHealth, the major data protection requirements for mobile applications are being discussed at European level (cf. no. 2.4).

Health apps must ensure data protection both in technical and in legal terms. This includes keeping in mind the data protection requirements already when developing health apps and related devices. Moreover, users must be fully and clearly informed about existing risks, e.g. the transmission of data to third parties. In addition to the voluntary commitments of manufacturers and awareness-raising among users of the risks involved in using health apps, I think that a legal framework is necessary as well. Regulators should protect consumer rights by imposing requirements on the use of apps and of the data collected through these apps, e.g. in a private health insurance fund. This also includes prohibiting the unauthorized linking, re-identification and analysis of these data by third parties.

For more information on this topic, please also refer to an issue of my publication "Datenschutz kompakt", available in German on my website at www.datenschutz.bund.de.

1.6 Government and corporate data protection officers

Data protection officers in businesses and government agencies play an extremely important role in applying and implementing data protection law. The combination of in-house controls in companies or public authorities and government supervision has been successful for decades. This two-pillar model is crucial for the relatively high degree of acceptance and the high level of data protection in Germany. In their authorities and companies, data protection officers provide staff and decision-makers with advice and practical assistance and monitor compliance with data protection law.

The underlying legal provisions in Europe and thus in Germany have developed in a very positive direction during the reporting period.

In the reporting period I focused on advising data protection officers in the federal administration and monitoring the legal and professional status of data protection officers in federal authorities.

Data protection officers under the General Data Protection Regulation

The General Data Protection Regulation (GDPR) introduced the two-pillar model across Europe. In Germany, we fortunately agree that we should use the discretion granted by the GDPR to maintain the almost full coverage with corporate data protection officers.

After long discussions, European regulators agreed that at least in certain cases, in-house data protection officers should be mandatory across Europe (cf. no. 1). This means that public authorities must always appoint a data protection officer. Exceptions apply only to courts in their judicial capacity.

Moreover, businesses must appoint a data protection officer if

- the core activities of the company consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities consist of processing on a large scale of sensitive data within the meaning of Articles 9 and 10 of the GDPR.

The legal status and tasks of the data protection officer specified in Articles 37 to 39 of the GDPR are similar to those specified in the Federal Data Protection Act (BDSG).

The Article 29 Working Party adopted corresponding guidelines providing valuable information about the appointment, legal status and tasks of data protection officers (Guidelines on Data Protection Officers adopted on 13 December 2016, WP 243 – available on my website at www.datenschutz.bund.de). I was heavily involved in drafting this paper and able to contribute my experience with the long-standing German system. The guidelines specify when data protection officers must be appointed, how they must be integrated into corporate/agency structures and with which status, when other tasks may cause conflicts, and which concrete tasks data protection officers have.

For businesses and public authorities in Germany, things will not change much, which in this case is good news. The GDPR directly obliges public authorities to appoint data protection officers. Article 37 (4) of the GDPR also allows member states to adopt national provisions going beyond the relevant provisions of the GDPR to oblige businesses to appoint data protection officers. In its bill amending data protection law, the Federal Government used its discretion to maintain the obligation to appoint data protection officers in its current scope (cf. no. 1.2.1). Fortunately, policy-makers, businesses and supervisory authorities agree that Germany should continue this policy.

Data protection officers in the federal administration

Data protection officers in the federal administration often ask me for advice on the practical implementation of the requirements of the Federal Data Protection Act. Moreover, I regularly find that federal authorities do not fully comply with the rules pertaining to government data protection officers.

Continued experience-sharing of data protection officers of supreme federal authorities – new guidance for government data protection officers

During the period covered by this report, I also continued the experience-sharing measures with data protection officers of the supreme federal authorities. Discussing common problems and unresolved legal issues is a good basis for the work of the data protection officers (cf. no. 12.2.4).
Since some questions kept recurring, I published a concept paper on minimum requirements for the organization and job description of data protection officers in the federal administration (*Mindestanforderungen an die Organisation und Aufgabenbeschreibung der behördlichen Datenschutzbeauftragten in der Bundesverwaltung*; cf. Annex 10 to my brochure “Info 4”)
These minimum requirements specify the function and independent position of data protection officers as well as the controller’s obligation to support the officers. In addition, they include many valuable recommendations on strengthening the data protection officers’ role, thus helping them perform their important task.

In order to assess the practical implications of the minimum requirements, I examined several federal authorities to see how they implement and comply with the legal provisions under Sections 4f and 4g of the BDSG. The results of this examination vary widely.

The controller's obligation to support the data protection officer

The overriding principle for the work of data protection officers is that they must not be subject to instructions in performing their tasks (Section 4f (3), second sentence, of the BDSG). In accordance with Section 4f (3), first sentence, of the BDSG, they must therefore be directly subordinate to the head of the public or private body to ensure that the organizational units they monitor cannot influence their activities. This secures the data protection officers' independent position and ensures that they can always directly report to the heads of their respective organization.

This also means that organizations must exempt their data protection officers from other official duties. Given their special status, the work as data protection officers must always take precedence in case of time overlap with other tasks (cf. Section 4f (3) of the BDSG).

I found that in practice, federal authorities often do not exempt their data protection officers from other tasks or only do so to a limited extent. In this respect, there is room for improvement in many organizations.

For example, I recommend that organizations with more than 1,000 employees exempt their data protection officers from all other tasks given the scope of the tasks related to privacy rights of employees. Depending on the scope and complexity of the processing of personal data or the sensitivity of the data, full exemption may be necessary even if the number of employees is lower.

When visiting authorities and talking to data protection officers at supreme federal authorities, I found that in practice, the special legal status of government data protection officers is not always sufficiently recognized, creating discrepancies between what is and what should be.

A public body has some organizational leeway to implement the necessary exemption from tasks, depending on the circumstances in the authority and the

specific needs of the data protection officer and his/her assistants. For example, it would be acceptable if the data protection officer is exempted 50% of the time and has an assistant who is also exempted from 50% of their tasks because together, this would equal full exemption. The aim must always be to ensure the necessary exemption from other duties and effective performance of data protection tasks (cf. no. 14.1).

Deputy data protection officer

While the BDSG does not provide for a deputy position, neither does it exclude this possibility. The deputy data protection officer is considered an “assistant” within the meaning of Section 4f (5) of the BDSG. Appointing several data protection officers would not be compatible with the independence of this office. Therefore, a deputy may be appointed only for times when the data protection officer is absent or otherwise prevented from carrying out his/her duties. The special rights granted by the BDSG, including special protection against dismissal and the right to refuse to give evidence, do not apply to assistants and therefore also not to the deputy data protection officer.

Data protection officers should not also be IT security officers

One of my tasks was to check whether a data protection officer can at the same time be the IT security officer. Especially in strongly IT-based companies such as telecommunications and postal services, both positions are related because both have to acquire knowledge about data collection, processing and storage. In particular, companies with a small workforce are therefore tempted to have one person fill both positions.

However, the two roles are potentially conflicting, e.g. when it comes to retention periods for personal data. Whereas, according to the Telecommunications Act (*Telekommunikationsgesetz*, TKG), the data protection officer of a telecommunications company has to call for restrictive storage, the IT security officer seeks long-term retention of data to be better able to detect and analyse disruptions. This is a serious conflict of interests. We only have to look at telecommunications

companies, for example, which regularly challenge the retention period of traffic data specified in the joint 2012 guidelines of the Federal Commissioner for Data Protection and Freedom of Information and the Federal Network Agency for privacy-friendly storage of traffic data. Finally, it is questionable whether a data protection officer could impartially examine a company's IT security strategy, for example, if he/she was the one who developed the strategy in his/her capacity as IT security officer.

To avoid conflicts of interest, I therefore generally recommend that the roles of data protection officer and IT security officer should be assigned to different persons.

External data protection officer – always a natural person

A person from outside the controller may also be appointed data protection officer (Section 4f (2), third sentence, first half-sentence, of the BDSG). Such person may only be a natural person, not a legal person or partnership company.

The requirements of "specialized knowledge" and "reliability" to be fulfilled by the data protection officer (Section 4f (2), first sentence, of the BDSG) and his/her freedom to use his/her specialized knowledge in the area of data protection without instructions (Section 4f (3), second sentence, of the BDSG) were written with natural persons in mind, which is logical. They also apply to data protection officers from outside the controller. If the data protection officer were a legal person or partnership company, data subjects who wish to contact the data protection officer in confidence could not be certain that the person contacted in fact would represent the matter and would continue to be an organ of the legal person, not least because the natural persons representing a legal person may change. Finally, a legal person is not able to maintain secrecy (Section 4f (4) of the BDSG); only natural persons can do this.

The GDPR, too, assumes that only natural persons can fulfil the requirements of "specialized knowledge" and "suitability". In its guidelines, the Article 29 Working Party (no. 1.6) accepts that an external data protection officer may also be a legal person. However, in this case each (natural) person who performs tasks of the data protection officer within this organization must fulfil all requirements for the

appointment of a data protection officer. Within a team, responsibilities should be clearly distributed, and one person should be appointed as the primary contact.

Term of office of the data protection officer

Data protection officers are appointed for an indeterminate period of time. In particular, Section 4f of the BDSG provides for neither a fixed term of office nor the possibility of a temporary appointment as data protection officer.

However, I and many others agree that a temporary appointment is nevertheless possible. Following the same legal pattern, the state data protection acts of Mecklenburg-Western Pomerania and Thuringia include provisions governing a limited or fixed term of office.

However, a limited term of office is unlawful when it prevents data protection officers from fulfilling their duties or violates protection under Section 4f (3) of the BDSG, which would apply in particular when the term of office is kept very short.

For example, a very short term of office would prevent the data protection officer from thoroughly examining particularly difficult cases and could also be used to undermine the protection from dismissal. Therefore, as a rule only a term of at least four years can be recognized as lawful. Shorter terms would require special justification and have to be necessary due to the special nature of the organization.

The limitation must not be subject to other conditions outside the term of office because the purpose of the special protective provisions is not compatible with conditions of dismissal.

Terminating the appointment of the data protection officer

In addition to the expiry of a limited term of office, the appointment of a data protection officer can be terminated only subject to mutual consent, by unilateral resignation or on the basis of the special provisions on revocation pursuant to Section 4f (3), fourth sentence, of the BDSG.

According to this provision, the appointment of a data protection officer may be revoked only if the prerequisites for termination without notice for compelling reasons pursuant to Section 626 of the Civil Code (*Bürgerliches Gesetzbuch*, BGB) are fulfilled. For this to apply, facts must be present on the basis of which the revoking party cannot reasonably be expected to continue the appointment, taking all circumstances of the individual case into account and weighing the mutual interests.

However, Section 4f (3), fourth sentence, of the BDSG has a different aim than Section 626 of the Civil Code because it does not protect an employee but the function of the data protection officer. Therefore, there may be cases where only the appointment of a data protection officer can be revoked but not the underlying legal relationship. However, the termination of the underlying work or service relationship is always a compelling reason to revoke the appointment.

Compelling reasons within the meaning of Section 4f (3), fourth sentence, of the BDSG are only those which refer to the function of the data protection officer and make further service impossible. This would apply if data protection officers permanently violated their monitoring obligations, seriously violated data protection law when performing their duties or had serious conflicts of interest.

2 European and international focus topics

2.1 The transition from Safe Harbor to Privacy Shield: Is it just the same old thing in a new guise or is there justified hope for legally secure transatlantic data communications?

Following the European Court of Justice's rescission of the European Commission's Safe Harbor decision, the discussion of data protection law focuses once again on the comprehensive and suspicionless surveillance activities by the U.S. intelligence services. It remains to be seen whether the new regulations known as the "EU-U.S. Privacy Shield" will create lasting legal certainty for transatlantic data communications.

The rescission of the European Commission's adequacy decision on the Safe Harbor arrangement (2000/520/EC) of 26 July 2000 by the ECJ's so-called Schrems judgment (6 October 2015, file ref. C-362/14) was a shock which will be felt for a long time. The complaint, which was filed with the Irish data protection agency by an Austrian citizen protesting against Facebook's transfer of his data to the U.S., resulted in a judgment which is in many respects a landmark decision.

The ECJ found for example that there was nothing in the European Commission's Safe Harbor decision to prevent the national control bodies from checking in a completely independent way whether data transmissions comply with the requirements defined in the Data Protection Directive (95/46/EC) to protect the fundamental right to data protection enshrined in Article 8 of the EU Charter of Fundamental Rights (the Charter). Not only did the ECJ considerably upgrade the role of the European data protection authorities, it also insisted that they be given the right to bring an action against Union legislation. I am eagerly awaiting the transposition of this judicial requirement into German law.

Furthermore, the ECJ declared the Safe Harbor decision as such to be null and void, stating that the European Commission had not ascertained with sufficient justification whether the U.S., based on national legislation or international commitments,

guarantees a level of protection which is essentially equivalent to the level guaranteed in the European Union.

Apart from this formal argument, the Court also refers to the legal situation and legal practice in the U.S. indicating those regulations governing the surveillance powers of public authorities and the legal redress options available to data subjects which, in the Court's view, constitute a particularly serious infringement of European fundamental rights.

The Court held, for example, that any regulation granting government agencies general access to the content of electronic communications violated the essence of the fundamental right to respect for private life enshrined in Article 7 of the Charter.

The Court also found that any regulation which does not provide citizens with the right to legal redress and thus give them a possibility to get access to their personal data or to have these data corrected or deleted constituted a violation of the fundamental right to effective judicial remedy.

All adequacy decisions of the European Commission and the alternative instruments for data transfers to countries that do not have an adequate level of data protection, such as standard contractual clauses and binding corporate rules (BCRs), will have to be measured against these requirements and this legal rationale.

This applies first and foremost to the rules replacing the Safe Harbor regime. With the European Commission’s decision (2016/1250) of 12 July 2016 and following intensive negotiations between the Commission and the U.S. government, the “EU–US Privacy Shield” now constitutes a new legal basis for data transfers to the U.S. in the form of an adequacy decision pursuant to Article 25 (6) of the Data Protection Directive (95/46/EC).

The intensive guidance provided by the Article 29 Working Party of the European data protection agencies throughout the negotiating process brought about many improvements. The rules governing data transfers to third parties for example have been designed to provide greater data protection and the concept of purpose

limitation, which is of central importance under European data protection law, has been enshrined in the EU–US Privacy Shield. I was substantially involved in developing the comments of the Article 29 Working Party.

In the version that has now been adopted, the EU–US Privacy Shield contains additional and in some cases substantial improvements compared to the former Safe Harbor regulation. Among other things, the new regulations provide for the office of an ombudsperson to be established within the U.S. State Department in order to receive complaints about possible surveillance activities of U.S. intelligence services and security agencies.
It should also be stressed that, in compliance with the requirements of the ECJ judgment, the previous restrictions on the powers of the completely autonomous European data protection agencies are no longer contained in the EU–US Privacy Shield.

From the perspective of data protection law, however, there are still some aspects of the EU–US Privacy Shield that merit criticism. These aspects include in particular the lack of concrete commitments on the part of the U.S. government regarding the limitation of mass surveillance and the question whether the ombudsperson is in fact able to ensure effective legal remedy as referred to in Article 47 of the Charter. In order to do that, the ombudsperson would not only have to be independent of the agencies subject to his/her supervision, but he/she would also need the powers to examine documents independently in order to form an opinion of his/her own and to take remedial action where necessary.

While the Article 29 Working Party continues to have reservations, it has decided to await the results of the first review of the EU–US Privacy Shield, which is to be carried out by the European Commission and the U.S. government at annual intervals, starting in 2017. The European data protection agencies strive to be actively involved in this review. I, too, will actively help shape this process.

It remains to be seen whether the already identifiable measures taken by the U.S. side will be sufficient to allay the concerns of the European data protection agencies, in particular when it comes to surveillance measures and legal redress.

Although only a few months have elapsed since the EU–US Privacy Shield became effective, several lawsuits have already been filed with the ECJ to challenge this decision by the European Commission. The use of standard contractual clauses for data transfers from the EU to the U.S. is also the subject of judicial review. These proceedings will also provide further insight into the framework conditions for transatlantic data communications and data transfers to other third countries.

2.2 Umbrella Agreement: The umbrella is open. Are there any holes in it?

The so-called Umbrella Agreement is in effect. Practice will show whether the options for EU citizens seeking legal redress against security agencies in the U.S. will actually improve.

After years of negotiations, the so-called Umbrella Agreement was concluded. The agreement does not create any new legal basis for the transfer of personal data to security agencies in the U.S.; instead it obliges the security agencies of the European Union Member States and those of the U.S. to comply, in the event of a data transfer, with the data protection standards laid down in the agreement. Apart from that, the transfer requires an independent legal basis on both sides. In other words: The agreement creates rights for data subjects and obligations for security agencies which consistently apply from now on and are no longer negotiable to the extent that the agreement applies. This qualification is relevant, because the standards do not apply in cases where intelligence services exchange personal data or where U.S. security agencies collect personal data of European citizens elsewhere, be it in the U.S. or in other parts of the world.

From the perspective of data protection law, this agreement can, however, become a success only if the legal protection afforded in the U.S. to European citizens actually improves. This lack of legal redress has been a burden on transatlantic security discussions for years and the ECJ also attached substantial importance to this matter in the so-called Schrems judgment (judgment of 6 October 2015, file ref. C-362/14; see also no. 2.1 above).

When my last activity report was published, the U.S. Attorney General at the time had announced that the U.S. administration intended to provide better legal redress for European citizens in the U.S. This announcement was followed by action. The U.S. Congress passed the Legal Redress Act, bringing the level of legal redress granted to European citizens at least closer to the level of redress granted to U.S. citizens. This means that while progress has been achieved, it is not yet clear how exactly the new regulations will affect security agencies. It is too early yet to answer that question. Regulations in the U.S. are complex, and practice will have to show to what extent the improved legal redress applies also with regard to the U.S. security agencies.

Like other security agreements concluded with the U.S., the Umbrella Agreement provides for a joint review to establish whether the agreed rules are being followed in the U.S. and how they are implemented. The Article 29 Working Party will be actively involved in this review. I attach great importance to the practical review of the agreement and will closely monitor the further developments.

I consider the agreement an important step towards setting standards for information sharing with the U.S. in the field of security that are binding and as high as possible. Although the agreement does not resolve all controversial issues, I nevertheless support the underlying approach. Agreeing on binding improvements to enhance the protection of data subjects in the context of transatlantic data transfers in the sensitive field of security is a lengthy and arduous process. If, however, the agreement turns out to be a success, it could well serve as a model for similar agreements with other countries.

2.3 Security, border management and data protection law challenges

According to the European Commission, there is a need to enhance the security of the external borders. The European Commission and the security agencies of the member states agree on this. This is why modernizing border management is high on the political agenda; however, privacy rights must not be ignored in this context.

With its Communication “Stronger and Smarter Information Systems for Borders and Security” of April 2016, the European Commission provided the strategic framework for a number of projects, including the introduction of an entry and exit system (EES), the introduction of a travel information and authorization system (ETIAS - cf. no. 2.3.1), the recast of the Eurodac Regulation (cf. no. 10.3.3) and the implementation of the Directive on the use of passenger name record (PNR) data (PNR cf. no. 2.3.2).

All these measures are driven by the desire to enrich existing information systems in the fields of border management, asylum and migration with data, to make the systems seamlessly usable on a reciprocal basis and also for purposes of threat prevention, law enforcement and counter-terrorism and to effectively fill any knowledge gaps (where they still persist) through additional systems.

The increasing system interconnectivity involves substantial interferences with the rights of data subjects and challenges data privacy law principles. It is imperative to preserve the key mechanisms that protect the individual’s privacy rights. These mechanisms include the principle of purpose limitation, data minimization, retention periods, access limitations and the ability to check data processing. For this reason, I will continue to keep a critical eye on the planned regulations.

2.3.1 Smart borders and interoperability – EES and ETIAS paving the way for interconnected border management

These acronyms stand for projects which aim to collect comprehensive information on persons crossing the Schengen borders. Data bases are to be interlinked, the data are to be retained for years on the grounds of general security considerations. Fundamental data protection principles are threatened.

The projects pursued under the heading ‘smart borders’ were already critically reviewed in my previous activity reports (24th Activity Report, no. 2.5.3.4, 25th Activity Report no. 3.3). The European Commission’s proposal for the introduction of an entry and exit system (EES) stipulates that in future, all border crossings by third–country nationals visiting the EU are to be centrally registered. In this context, bio-graphical data, fingerprints, biometric facial images and information on border

crossings and refusals of entry (so-called entry-exit-records) are to be processed. The system is to be linked to the Visa Information System (VIS) so that border authorities can immediately access the VIS from the EES and all data will only have to be stored just once. Visa and asylum authorities are to be given access to the EES for the purpose of processing pending cases, while the law enforcement and intelligence services are to be given access for the purpose of preventing and prosecuting terrorist and other serious criminal offences.

The principle of purpose limitation is called into question by the comprehensive access rights including those accorded to the intelligence services and the interconnected access to various databases. This creates a system which on a massive scale collects data on third–country nationals crossing the Schengen borders and stores them for years on the grounds of general security considerations. Given the complex processes within the EES it seems after all rather doubtful whether the database will actually be able to fulfil its primary purpose, which is to facilitate border checks. Also, there are considerable concerns as to whether setting up a large-scale database with biometric data for the purpose of simplifying procedures is in line with the principle of proportionality.

According to the proposal for the introduction of a European Travel Information and Authorisation System (ETIAS), all third–country nationals who are exempt from a visa requirement would have to obtain a travel authorization through ETIAS before they enter the Schengen area. This procedure is intended to permit an early assessment of security threats, migration risks and health hazards. For this purpose, biographical data including data on the traveller’s level of education and current employment as well as his or her replies to various background questions and the IP address from which the application was filed, are to be collected. Under the largely automated approval procedure, the data are to be subsequently checked against all relevant EU-wide travel, asylum and police information systems including specific threat indicators and a checklist. In the event of a match, the decision on the application will be taken manually. Apart from the approval and border control authorities, the security authorities in particular will have access to these data for the purpose of preventing and prosecuting terrorist and other serious criminal offences.

The proposed system may help to avoid refusals of entry at the external border and facilitate border checks in that respect. Apart from that, however, it is doubtful whether the system is actually suitable for filtering out individuals who represent a security, migration or health risk. So far, no convincing examples have been presented. The general reference to good experiences in other countries is not convincing in this context. This holds true in particular where the scope of data collected even exceeds that of the data collected in the context of the visa procedure. Here the question arises as to why travellers who are exempt from a visa requirement should be asked to provide more data than travellers applying for a visa. Nor has the need for the planned access rights of the security authorities yet been convincingly demonstrated. As under the proposal for the introduction of an Entry-Exit-System (EES), data of individuals wishing to enter the Schengen area are to be retained for several years as a merely precautionary measure. The planned matching function on the basis of the IP addresses offers numerous options for data linkage.

The European Commission is pursuing further networking options with the aim to ensure interoperability. The European Commission's long-term vision is to merge the relevant information systems in the fields of border management, migration and law enforcement into a new overall system consisting of a central identity database (core module) and specialized modules that are linked to the core module.

I view the plans for such a core module with great concern. From there it is just a short step to an EU-wide population database. Such a system would hardly be compatible with European data protection law. It would pose a significant threat to fundamental principles such as purpose limitation, the right to deletion/right to be forgotten, ability to check, data minimization and data austerity ('need to know').
In a letter addressed to the Council, the Commission and the European Parliament, the Article-29-Working Party also voiced its criticism concerning EES, ETIAS and interoperability.

2.3.2 Passenger Name Records: The next chapter

After years of negotiations, the European Union has adopted a Directive on the collection and storage of passenger name records (PNR data) for security purposes.

While the governments of the member states are already preparing the implementation, the focus is on the European Court of Justice in Luxembourg.

This matter has been on my mind for a long time already. In my 22nd Activity Report (no. 13.5.3), I reported on initial proposals aimed at using so-called passenger name records (PNR data) for security purposes and storing them for years. These are data records generated by airlines for the purpose of transporting passengers. The PNR Directive now obliges the airlines to transmit these data to a security authority even before take-off.

The European Parliament in particular long viewed this project with scepticism, but under the impression of the horrific terror attacks in Brussels and Paris the European legislators ultimately adopted the Directive in April 2016. The Directive stipulates that each member state has until May 2018 to set up a Passenger Information Unit which collects PNR data and stores them for five years; according to the ministers for home affairs this applies to all flights which are not purely national flights.

The PNR system essentially has a two-fold purpose. Firstly, it serves to check all airline passengers against abstract threat patterns. An airline passenger will be singled out for a check at the border if he meets certain criteria matching those of criminal offenders arrested in the past (e.g. mode of booking, flight route chosen etc.). The Directive is therefore expressly aimed at targeting specific passengers who are not suspected but whose PNR records follow a specific threat pattern. While the Directive stipulates that the decision on the concrete check at the border always has to be taken by an officer, the pre-selection will in future be based on the patterns defined by the computer program.

The second major purpose of the PNR system is to use the stored data for the purposes of preventing and prosecuting terrorist and serious criminal offences. As in the case of data retention, the passenger name records are to be stored for a period of five years irrespective of any suspicions; after a period of six months, however, they are to be “depersonalized”. After that, access to the full data record will be permitted only if a judge arrives at the conclusion that access to the data is necessary in the individual case to prosecute serious criminal offences.

In order to understand the extent of data storage to be expected in Germany, it is helpful to take a look at the following figures. According to information provided by the Statistical Office of the European Union, approximately 164 million air passenger name records would have been analysed and stored in 2014. This number is so high essentially due to the declared intention of the European home affairs ministers to apply this regime also to flights which originate and terminate within the European Union. According to the Directive, it is not mandatory to include such flights in the system. For Germany this means collecting PNR data for almost 100 million more passengers than if only flights originating or terminating in third countries were included.

My original scepticism has not been allayed: Based on the Directive, the member states will build up huge databases while the arguments presented to justify the need for data collection on that scale are rather vague. I do acknowledge that, in the course of the years of negotiations, a number of additional procedural safeguards have been included in the Directive to ensure compliance with the principle of proportionality. These safeguards include the principle that data are to be depersonalized after a period of six months, the provision that data access will be subject to a special authorization after that period and the rule that certain sensitive data must not be used as a basis for matches against threat patterns.

In the process of transp0osting the Directive into German law, I will seek to ensure that the existing latitude is used to enhance data protection. In this context, I will continue to focus on the European Court of Justice in Luxembourg. As far as passenger name records are concerned, I referred already in my last activity report to the ECJ's rulings on measures that potentially interfere with fundamental rights, noting that the Court's case law corresponds increasingly to that of Germany's Federal Constitutional Court. The ECJ will have the final say when it comes to deciding whether and to what extent the European Passenger Information Units should be allowed to analyse and store personal data in the absence of any suspicion. After the ECJ invalidated of the Data Retention Directive (2006/24/EC), the European Parliament asked the ECJ for an expert opinion to assess the

lawfulness of an agreement that is to govern the transfer of PNR data on a similar basis to the Canadian security authorities.

2.3.3 Schengen evaluation in Germany

The expert group to review the implementation of the Schengen acquis also reviewed my activities.

Already in summer 2015, an expert group reviewed the implementation of the so-called Schengen acquis in Germany. The group was composed of European Commission representatives and of experts despatched by the member states' data protection commissioners. In the context of their review, the group examined the extent to which institutions in Germany contribute to an efficient implementation of the Schengen area and the relevant legal acts (Regulation (EU) no. 1053/2013 of the Council of 7 October 2013, Article 2). This review concerned not only my activities and those of the data protection commissioners at state level but also the activities of the data protection officers at the Federal Police, the Federal Criminal Police Office and the Federal Foreign Office.

In my remit, the review extended among other things to my monitoring and advisory activities regarding the Schengen Information System, the Visa Information System and border management projects. This includes the support I gave in response to requests from data subjects and information materials on these matters that were provided by my agency.

Another key aspect of the review concerned my independence which had been called into doubt at the last Schengen evaluation. Since I have been completely independent since 1 January 2016, this important prerequisite is now finally met.

In accordance with the expert group's preliminary review report, I believe that all the demands imposed on me are met. It should be pointed out, however, that in order to meet the demands imposed on me I should have a sufficient number of staff. This is necessary also in order to comply with the requirement that reviews be conducted at

intervals of no more than four years and with the necessary diligence and in order to respond to information requests by data subjects within an appropriate timeframe.

2.4 Data protection at EU level – driven by the Article 29 Working Party and its subgroups

The Article 29 Working Party actively promotes uniform and effective data protection in the European Union.

In 2015 and 2016, the Article 29 Working Party once again dealt with a broad range of different topics. It adopted six official opinions, statements and other working papers on current data protection issues. Topics addressed included the reform of European data protection legislation (cf. no. 1) and the revision of the data protection framework in the transatlantic relationship between the EU and the U.S. (cf. no. 2.1, no. 2.2).

A list of the opinions and documents adopted by the Article 29 Working Party in the reporting period is available on my website at www.datenschutz.bund.de.

Action plan for the implementation of the General Data Protection Regulation

After the European Parliament and the Council had agreed on the new EU data protection legislation (cf. no. 1.1), the Article 29 Working Party began preparing for their practical implementation. In its 104th plenary session in February 2016, it adopted an action plan for the implementation of the General Data Protection Regulation (GDPR). In this context, the Future of Privacy, Key Provisions and Cooperation subgroups focused on the structure of the future European Data Protection Board – the successor to the Article 29 Working Party – and on the new procedure for cooperation between supervisory authorities in cross-border cases. The Article 29 Working Party developed guidelines and working papers on the following topics:

- carrying out the one-stop shop and the consistency mechanism, and interpreting relevant legal terms of the GDPR (e.g. the term “main establishment”);

- mutual assistance, joint measures and cooperation between authorities in cross-border cases;

- determining the lead supervisory authority in one-stop-shop cases;

- corporate and government data protection officers;

- right to data portability.

I was actively involved in the work of the Article 29 Working Party. This applies in particular to the guidelines on the lead authority and on data protection officers, for which I was co-rapporteur in the Key Provisions subgroup. In my capacity as co-rapporteur, I also participated in drafting the rules of procedure of the European Data Protection Board, work which will be continued in 2017. The Article 29 Working Party decided to develop another action plan for implementing the GDPR and for preparing the work of the future European Data Protection Board.

Data protection in the area of police and judicial cooperation and of border controls

In addition to monitoring the EU data protection reform, the Article 29 Working Party took a detailed look at the security area from a data protection perspective. The Working Party's efforts were dominated by the negotiations between the EU and the U.S. on the Privacy Shield (cf. no. 2.1). The Border, Travel, Law Enforcement (BTLE) subgroup, in which one of my staff members acts as a coordinator, elaborated the key fundamental rights and data protection standards for carrying out surveillance measures as described in the rulings of the European Court of Justice and the European Court of Human Rights. On this basis, the subgroup analysed the U.S. legal practice. The evaluation of European rulings is summarized in working paper 1/2016 "European Essential Guarantees" of the Article 29 Working Party. The analysis of U.S. law makes up a major part of the opinions of the Article 29 Working Party on the EU-U.S. Privacy Shield (opinion 1/2016 on the EU-U.S. Privacy Shield adequacy decision, cf. no. 2.1).

Moreover, the BTLE subgroup prepared many opinions of the Article 29 Working Party on other legislative projects. This includes the EU-PNR Directive (cf. no. 2.3.2), the Smart Borders programme (cf. no. 2.3.1), the Umbrella Agreement (cf. no. 2.2) and the Data Protection Directive for the area of police and justice (cf. no. 1.1, no. 1.2.2).

In the reporting period, the Article 29 Working Party also addressed the question whether and under which conditions security authorities may access data which are not stored on domestic servers. This problem is particularly urgent in times of globalization, the Internet and data storage in “clouds”. As I have already mentioned in my last report (cf. 25th activity report, no. 4.7.1), very important court proceedings on this matter are underway. The proceedings were initiated by Microsoft. At the request of a U.S. security authority, the company was obliged to disclose data on a customer’s e-mail account stored on servers in Ireland. A U.S. appeals court ruled that the U.S. government must ask for legal assistance to access the data stored in Ireland. According to the appeals court, applicable U.S. law does not allow authorities direct access. A final court decision is still pending, and also the general question of whether authorities are allowed to access personal data stored abroad must be addressed by all legal systems.

International tax information exchange and money laundering

The Article 29 Working Party also discussed the topic of automated sharing of international tax information (cf. no. 8.2.4) and the amendment of anti-money laundering legislation through the Fourth and Fifth EU Anti-Money Laundering Directive (cf. no. 8.2.2). Anti-money laundering discussions focus on transparent cash flows and the question of how and to what extent cash payments should be maintained. In this context, I participated in a consultation on a study initiated by the European Commission. Its results will be translated into proposals for future EU legislation.

Data protection in e-government

Finally, the Article 29 Working Party is examining the Code of Conduct on privacy for mHealth which introduces a system of voluntary commitment and is especially targeted at developers and producers of mobile health applications. The Code of Conduct was submitted to the Article 29 Working Party in June 2016. The E-Government subgroup is currently consulting with the authors of the Code of Conduct to improve the level of data protection. On the basis of this document, the major data protection requirements for mobile applications are being discussed at European level (cf. no. 1.5).

Data protection and new technologies

The Technology subgroup of the Article 29 Working Party drew up a recommendation on the use of drones (cf. no. 10.2.6) and an opinion on the revision of the ePrivacy Directive (EU Directive on privacy and electronic communications; cf. no. 17.2.4.1).

Coordinating national enforcement measures

The Enforcement subgroup reactivated in late 2016 will have the task of coordinating the other subgroups and harmonizing the relevant procedures in the context of the necessary national enforcement measures. The messaging service WhatsApp was the subgroup's first project. After the service had been acquired by Facebook, the Article 29 Working Party asked WhatsApp in writing to refrain from transmitting personal data of EU citizens to Facebook. In response, WhatsApps has temporarily suspended data transmission until all legal issues are resolved (cf. no. 17.3.1).

2.5 Council of Europe

Progress in revising Data Protection Convention 108

The globalization of data flows has led not only to the modernization of European Union data protection legislation; since 2009 also the Council of Europe has been

revising the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). In the reporting period, significant progress has been made in the negotiations on an amending protocol. However, final agreement is still pending.

After EU consultations on the General Data Protection Regulation had been concluded (cf. no. 1.1), work on revising Convention 108 made considerable progress (cf. 24th activity report, no. 2.4.3). In June 2016, the Ad-hoc Committee on Data Protection (CAHDATA), responsible for revising Convention 108, forwarded a draft amending protocol to the Rapporteur Group on Legal Cooperation (GR-J) of the Council of Europe. The group will discuss the points on which CAHDATA could not reach consensus to prepare adoption by the Committee of Ministers. Despite intensive efforts, the Rapporteurs Group was not able to reach full consensus on the amending protocol by late 2016. One reason was that the Russian Federation asked for more exceptions for data processing for the purposes of national security; another was that EU member states had different views on the future voting rights of the European Commission in the Consultative Committee (T-PD) and on how the amending protocol should enter into force. Despite these unresolved issues, I welcome the significant progress made in revising the Convention. This applies primarily to its scope of application which covers the entire public and private sector. I am pleased that the Federal Government did not endorse the request of the Russian Federation to fully exempt data processing by intelligence services from the Convention's scope of application. Another positive aspect is that concerning the basic data protection principles, the data subjects' rights and the obligations of the controller, the amending protocol is largely in line with the principles of the EU General Data Protection Regulation and the EU Data Protection Directive so that the necessary consistency between the Convention and the new EU legal framework has been achieved. Another important improvement for data protection is the amending protocol's requirement that the contracting parties should establish independent national supervisory authorities which can monitor compliance with data protection rules and sanction non-compliance, and which cooperate and provide mutual legal assistance in implementing the Convention.

In 2016, the Federal Ministry of the Interior – the lead authority in this area – allowed me to participate in Council of Europe meetings which touch upon data protection, a request I had made for many years. I may now participate as an observer in the meetings of CAHDATA and the Consultative Committee pursuant to Article 18 of Convention 108 (T-PD). In the T-PD, the interior ministry also allowed me to speak freely as a representative of independent data protection supervision in Germany. I am pleased about these opportunities and actively take advantage of them. This applies to interministerial coordination as well as to work in the TP-D plenary to improve the guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, discussed by the TP-D in 2016, and recommendations on the protection of personal health-related data .

2.6 International Conference of Data Protection and Privacy Commissioners

In the reporting period, two international conferences of data protection and privacy commissioners addressed key issues of the future and initiatives to improve global cooperation.

The 37th International Conference of Data Protection and Privacy Commissioners in Amsterdam (26-29 October 2015) focused on “privacy bridges”. Shortly before the conference started, the need to build privacy bridges between the EU and the U.S. became even more important after the European Court of Justice had revoked Safe Harbor in the so-called Schrems decision (cf. no. 2.1).
Challenges posed by processing health and genetic data and questions regarding the role of data protection supervisory authorities in the context of surveillance by intelligence services were further major topics at the conference. Three resolutions were adopted: In addition to the Resolution on Transparency Reporting and the Resolution on Privacy and International Humanitarian Action, the Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy deserves special mention. This resolution – introduced by me – is based on a German-Brazilian initiative at the United Nations on the right to privacy in the digital age. Following this initiative, the General Assembly of the United Nations adopted two resolutions (68/167 of 18 December 2013 and 69/166 of 18 December 2014). They formed the basis for the decision of the UN Human Rights Council of 26 March 2015

to appoint a Special Rapporteur on the right to privacy. His task is to submit an annual report on violations of the right to privacy which is enshrined in the Universal Declaration of Human Rights and in the International Covenant on Civil and Political Rights of the United Nations. The Special Rapporteur is also supposed to follow international discussions on the right to privacy. In summer 2015, Professor Joseph Cannataci of Malta University was appointed Special Rapporteur for a period of three years.

The 38th International Conference of Data Protection and Privacy Commissioners in Marrakesh (17-20 October 2016) was held under the title “Opening New Territories for Privacy”. Discussions focused on the challenges associated with current developments such as robotics, artificial intelligence and machine learning, in particular for informational privacy of the individual and for the further course of data protection. Given the growing international data flows, participants also discussed encryption as an increasingly important instrument to protect personal data. Moreover, they adopted resolutions on a competency framework for school students on data protection, on developing new metrics of data protection regulation, on human rights defenders and on further developing international cooperation of data protection supervisory authorities.
A new working group was established to review the strategy, size and effectiveness of the International Conference, and I will actively contribute to this work. This also applies to an expert group on strengthening cross-border cooperation of supervisory authorities.
The resolutions of the International Conference of Data Protection and Privacy Commissioners are available in English on my website (www.datenschutz.bund.de).

The 39th International Conference of Data Protection and Privacy Commissioners will take place in Hong Kong on 25-29 September 2017.

2.7 Conference of European Data Protection Authorities

In 2015 and 2016, the annual Spring Conference of European Data Protection Authorities focused above all on the practical implementation of data protection in Europe and the new European General Data Protection Regulation.

The Conference of European Data Protection Authorities is traditionally held in April or May every year and is thus known as the Spring Conference to distinguish it from the International Conference of Data Protection and Privacy Commissioners, which regularly takes place in autumn (cf. no. 2.6). The Spring Conference offers a forum for sharing ideas and experience among all the data protection authorities in Europe and with representatives of the European Commission, the Council of Europe and the OECD; it is thus broader than the data protection panels of the European Union. In particular, it includes data protection officers from the countries of south-eastern Europe.

Under the title “Navigating the Digital Future”, the Spring Conference organized by the British data protection authority ICO in Manchester on 18-20 May 2015 focused on the practical implementation of data protection. Various forums discussed the expectations of citizens regarding the enforcement of their rights and the possibilities of organizations and data protection authorities to support citizens in this respect.

The dominant topic at the Spring Conference in Budapest on 26-27 May 2016 was the implementation of the General Data Protection Regulation at European and national level and its relation to Council of Europe Convention 108. Many participants called for harmonizing national provisions, finding Europe-wide approaches and strengthening cooperation. They stressed the benefits of European guidelines and standards for implementing the GDPR and advocated harmonization of national provisions as well as agreement on Europe-wide approaches.

The resolutions adopted at the 2015 and 2016 Spring Conferences are available on my website at www.datenschutz.bund.de. The next Spring Conference will be held in Limassol on 27-28 April 2017 and hosted by the Cypriot data protection authority.

8.2.1 AnaCredit – toward a common credit register

AnaCredit (Analytical Credit Datasets) is a project of the European Central Bank (ECB) to establish a granular and thus tailor-made credit reporting system. Unlike several other countries in the euro area, Germany is currently not operating a credit register. This project will become relevant from a data protection perspective as soon as data of natural persons are to be processed.

Starting in September 2018, Regulation (EU) 2016/867 of the ECB of 18 May 2016 on the collection of granular credit and credit risk data (ECB/2016/13) will require all banks to submit detailed debtor data. The AnaCredit Regulation must be distinguished from Regulation 2014/17/EU of the European Commission on credit agreements for consumers relating to residential immovable property, which has already been implemented in national law and governs the obligation to assess creditworthiness in the context of consumer credit agreements (Sections 505a and 505b of the Civil Code).

The ECB intends to introduce the EU-wide central credit database in two steps, but so far has specified only the first stage. The first stage does not yet involve reporting of credit data of natural persons; only data of legal persons will be required. However, it looks as though the scope of AnaCredit will be expanded to include natural persons in the second stage of implementation. Therefore, I am already following the project today.

Data to be reported include the amount, term, interest, currency, etc. of the loan. Up to 26 debtor attributes must be reported, including name, head office, legal form, size, sector, economic activity and other identifiers. Credit institutions resident in the euro area and branches of foreign banks located in the euro area must report the identifiers monthly to their respective national banks, which forward the data to the ECB. In Germany, the reports will be collected and forwarded to the ECB by Deutsche Bundesbank.

With the AnaCredit Regulation, the ECB wants not only to provide a standard method for collecting data on loans in the euro area, but also to significantly expand the

group of reporting agents in order to use these data to manage monetary risk and monitor financial stability. In Germany, for example, only large loans are reported to banking supervision, whereas in Portugal the reporting threshold is very low. However, Deutsche Bundesbank decided to ease reporting requirements for small institutions.

Data collection through AnaCredit is rounded out by the Act Complementing Supervision Law planned by the Federal Ministry of Finance. This legislative project is based on a recommendation of the Financial Stability Committee of 30 June 2015. The act will grant the Federal Financial Supervisory Authority (BAFin) the power to impose restrictions on granting loans for building or buying domestic residential real estate, if necessary to prevent a disruption of our financial system or financial stability.

I will continue to monitor this project in the Article 29 Working Party and at national level and work towards compliance with data protection rules in the second stage which will also involve collecting data of natural persons.

8.2.2 Implementing the Money Laundering Directive – a long-term task

On 20 May 2015 the European Parliament and the Council adopted the Fourth Anti-Money Laundering Directive.

The Fourth Anti-Money Laundering Directive is intended to create a consistent regulatory framework to fight money laundering and terrorist financing. For the first time, a transparency register will be put in place on the basis of this directive. This public register will contain information on the beneficial owners of corporate entities. Moreover, the directive now covers all gambling services (not only casinos) carrying out transactions amounting to 2,000 euros or more. It also provides for a lower threshold for commercially traded goods and a larger group of obliged entities.

The previous threshold for cash payments subject to reporting obligations was 15,000 euros. With the implementation of the Fourth Anti-Money Laundering Directive, member states are required to reduce this threshold to at least 10,000

euros, and national legislation can provide for even lower thresholds. However, defining national thresholds must not result in cash payments for expensive everyday goods such as tablets, computers or TVs being subject to anti-money laundering efforts and to the collection, transmission, storage and analysis of related data. Everyday expenses should not come under general suspicion of money laundering or terrorist financing. Citizens must continue to be able to buy everyday items without data collection.

Even before the implementation of the Fourth Anti-Money Laundering Directive in national law, on 5 July 2016 the European Commission submitted a proposal for a Fifth Anti-Money Laundering Directive. The Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC is intended to prevent the financing of terrorist activities. To this end, central Financial Intelligence Units would be given access to information in central registries for bank and payment accounts and to electronic data retrieval systems. For the first time, bodies exchanging virtual currencies would also be involved in the fight against money laundering and terrorist financing. In addition, the threshold for anonymous payments, e.g. with pre-paid cards, would be reduced from 250 euros to 150 euros, and stricter customer verification requirements would apply. Public access to the new transparency register would also be expanded.
The central Financial Intelligence Unit (FIU) – which will become part of the Customs Criminological Office – would be given more powers. The new directive would allow an analysis of reports submitted long before a threat or crime can be suspected, also when more data are added. The current proposal does not limit the specific means and scope of such analysis. Nor are the obligations of other authorities to provide information to the FIU subject to many restrictions. There is even an obligation to set up a mechanism for the automated exchange of data. This may entail significant changes of purpose. As a rule, the data would have been collected without the data subjects' knowledge. The legislation would even prohibit informing the data subject. This means that in principle, the Federal Constitutional Court requirements for using data from covert encroachments upon informational rights would apply (cf. no. 1.3). Together with the proposed amendment of the Customs Investigations Service Act

(*Zollfahndungsdienstgesetz*, ZFdG), the proposed directive would have implications for the protection of fundamental rights.

I will continue to follow the process in a spirit of constructive criticism, at European level through my participation in the Article 29 Working Party and with regard to its implementation at national level.

8.2.4 International exchange of tax information – Data must be processed within the EU

While sharing international tax information is undoubtedly necessary, data protection standards must be preserved as well. In view of the U.S. Patriot Act, data must be exchanged on European servers to prevent U.S. authorities from accessing tax information for other purposes.

The Panama Papers published in April 2016 once again illustrated the global nature of tax evasion and at the same time the relevance of the OECD standard for automated exchange of financial account information. With increasing globalization of investments and thus untaxed income, international cooperation between tax authorities is certainly essential. However, this international exchange of tax information must also abide by data protection standards. In Germany, the OECD standard was implemented in national law through the Act on the Automatic Exchange of Financial Account Information in Tax Matters and Amending Other Acts (*Gesetz zum automatischen Austausch von Informationen über Finanzkonten in Steuersachen und zur Änderung weiterer Gesetze*) of 21 December 2015 (Federal Law Gazette I no. 55, p. 2531). However, regulators did not fulfil my request to reduce the retention period of the data transmitted to the Federal Central Tax Office from 15 to ten years. The Federal Ministry of Finance was not able to convince me of the necessity of such a long retention period. Moreover, the act does not explicitly take into account my proposal to apply the data protection principles of necessity and data minimization to data collection by financial institutions as provided for in Section 6 (1) of the act. However, the act reflects my requests by incorporating the data protection principle of purpose limitation, according to which data may be used only for tax purposes.

Preparations for the first international tax information exchange, scheduled for September 2017, have started. In recent months, I have helped the Article 29 Working Party develop guidelines, in particular for sharing tax information with third countries. I also asked that the exchange be carried out on a European server. In this context, the initial idea was to use the server which is already being used for bilateral tax information exchange between the U.S. and Germany (under the Foreign Account Tax Compliance Act, FATCA, cf. 25th activity report, no. 7.5) also for the international OECD tax information exchange. I think that this is highly problematic from a data protection perspective because the U.S. Patriot Act gives U.S. authorities unlimited access to these data also for other purposes. Therefore, I will continue to insist that international tax information exchange should take place on European soil.

10.2.11.5 The standard data protection model

Work on the standard data protection model (Standard-Datenschutzmodell, SDM) has continued. Efforts were initially directed at defining suitable protection goals and procedures to create data security.

Protection goals and an IT security management based on these goals have been used in the field of IT security for many years, e.g. in the IT security assessment criteria, the Orange Book and the Common Criteria. However, implementation also exposes the shortcomings of these procedures and protection goals. For example, protection goals are not structured so that over time, a confusing array of parallel protection goals has developed and continues to develop. The various procedures also do not address the interaction between the protection goals, i.e. whether and to what extent they are mutually reinforcing, weakening, implicit or exclusive. Due to this lack of harmonization, there is no overview of the individual protection goals, and it is not possible to assess whether they are complete.

After many years of testing such procedures, in the mid-1990s the Federal Office for Information Security (BSI) developed the baseline security model (*IT-Grundschutz*) to make implementing such procedures easier. *IT-Grundschutz* has since become a practical tool to ensure IT security. The procedure is based on a simple model (cf. Box a on no. 10.2.11.5).

Although the BSI is currently revising *IT-Grundschutz*, the underlying principles will not change. In my 15th activity report (no. 30.8) I welcomed the baseline security model and summarized it in a simple formula:

DATA PROTECTION = baseline security + X

Over the years that this formula has been used, we often discussed how the X component can be determined and which “value” would be appropriate. Of course, this depends on the specific framework conditions, systems, data, etc. and so far could be defined only on a very basic level.

We therefore established a working group of the conference of independent federal and state data protection authorities already many years ago. The working group has adjusted its mandate on the basis of the baseline security model and developed the standard data protection model (SDM) with six goals.

The “classic” SDM goals include:

1. availability,
2. integrity, and
3. confidentiality.

As I explained in my 25th activity report (no. 5.14.1), these goals are not sufficient to ensure data protection and data security. Therefore, the following goals are needed as well:

4. non-linkability,
5. transparency, and
6. intervenability.

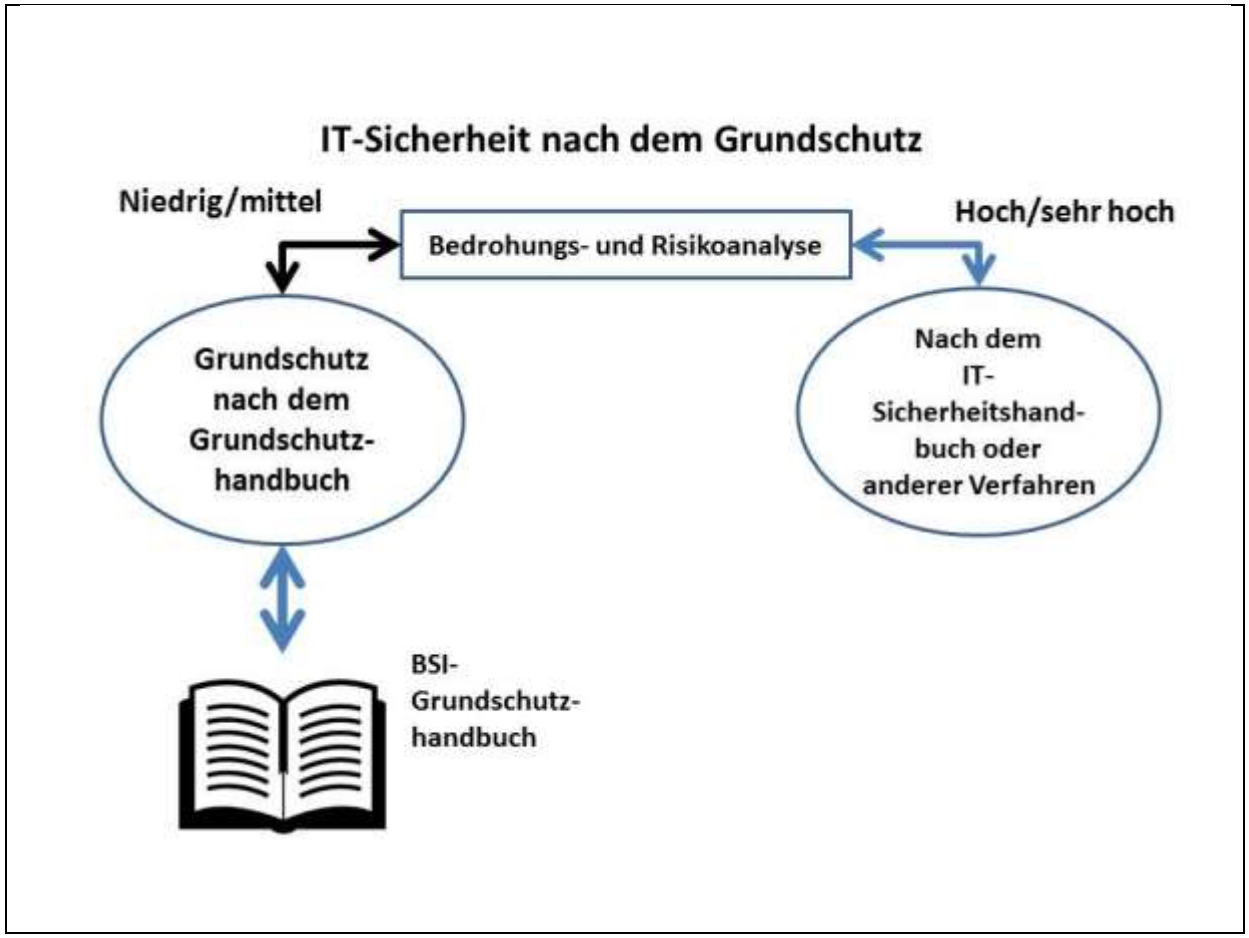
These six goals and the related measures may help determine the X component in the above formula. At the same time, this model complements the BSI’s baseline security model in an ideal way and uses the same method (cf. Box b on no. 10.2.11.5).

The SDM offers further advantages when looking at the soon-to-be applicable General Data Protection Regulation (GDPR).
The SDM goals transpose the legal requirements of the GDPR into the catalogue of technical and organizational measures required by the Regulation. Moreover, this reference catalogue can be used to review the effectiveness of the measures. Such standardized catalogues of measures are a good basis for data protection certification as provided for in the GDPR.
This standardization also supports the cooperation among supervisory authorities required by the Regulation which accompany the modern procedures for automated processing of personal data using uniform advisory and review strategies. The SDM

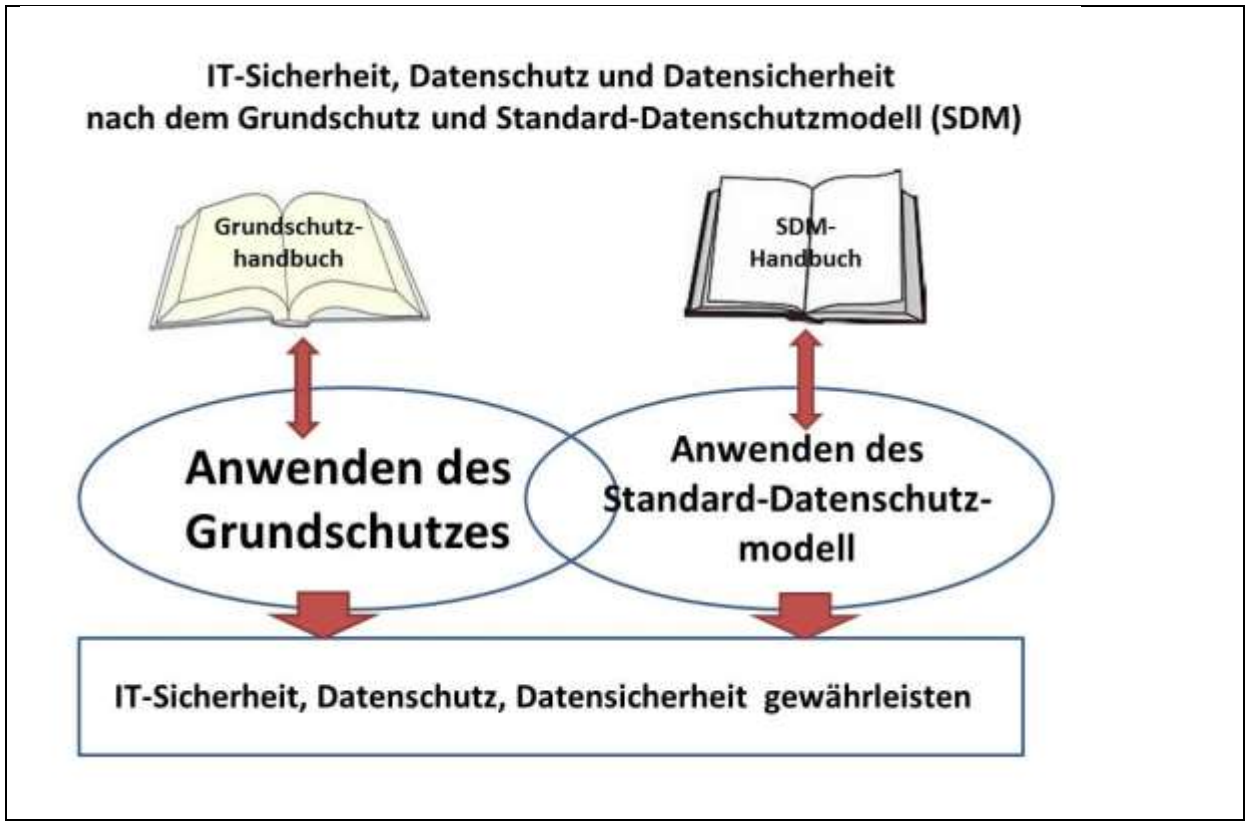
as a holistic review and advisory strategy can lead to a coordinated, transparent and verifiable system of data protection assessment.

The SDM should now be tested in practice, and a catalogue of measures similar to the one for the baseline security model should be prepared. In the framework of SDM version 1.0 (available at www.datenschutz.bund.de) several measures have been developed which can be directly applied. However, they must always be adapted and enhanced to keep pace with technological development. New technologies will entail new measures. In the future, the model will make an important contribution to data protection supervision in both the private and public sector in order to ensure data protection driven by fundamental rights.

Box a on no. 10.2.11.5



Box b on no. 10.2.11.5



10.3.3 The European fingerprint database for asylum seekers – Eurodac

Checks of the Eurodac database at the Federal Criminal Police Office (BKA) as the National Access Point revealed small errors which may be considered "teething troubles" in using the new system. I expect that the number of requests, which is very low at the moment, will significantly increase in the future.

In July 2015, the European Regulation (EU) No 603/2013 on the establishment of Eurodac for the comparison of fingerprints entered into force (cf. no. 22.11). The fingerprint database is intended to ensure effective application of Regulation (EU) No 604/2013 which defines which member state is responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person. At the same time, the Eurodac Regulation specifies under which conditions and how the member states' **law enforcement authorities** and Europol may lodge requests for **comparisons with Eurodac data**. The Eurodac database is operated by the European Agency for the Operational

Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

The Regulation provides for operating units in the member states which are authorized to request comparisons with Eurodac data. Only designated law enforcement authorities of member states can become operating units. A verifying authority examines the operating units' requests to assess whether the conditions for access as established in the Regulation are fulfilled. In case of compliance, the request is forwarded to eu-LISA via the **National Access Point**.

According to the Eurodac Regulation, **every year** an independent body must **audit** the processing of personal data for law enforcement purposes, including an analysis of a random sample of reasoned electronic requests. The first time I carried out such an audit was at the Federal Criminal Police Office (BKA) in 2016. The BKA was a suitable candidate because it is the National Access Point and has a verifying authority and operating units as specified in the Eurodac Regulation. Operating units within the BKA are certain divisions which are particularly suited for that role due to their responsibilities (preventing, detecting and investigating terrorist or other serious criminal offences).

Since the Regulation entered into force, the BKA as the National Access Point has forwarded 20 requests to Eurodac, of which 11 were its own requests. Three of the 11 BKA requests were forwarded on behalf of federal states which at that time were not yet able to submit requests themselves.

I inspected the workflows and procedures and also carried out random checks of requests. I only found minor mistakes which can be attributed to the fact that staff have not yet been sufficiently familiar with the procedure because of the low number of requests. Upon my announcement to inspect the BKA, the authority organized another series of training courses and considered adjusting workflows to rectify the identified shortcomings. I was pleased to note that no substantial errors were made. The requirements of the Regulation, e.g. previous consultation of other, higher-ranking databases, have always been met.

I expect that the number of requests and thus my supervision efforts will significantly increase. On the one hand, the procedure is still quite new, and both entering and requesting data needs more practice. On the other hand, the European Commission

already has concrete plans to **expand Eurodac's scope of application** (cf. no. 2.3.1). For example, the Commission wants to allow member states to store and search data of third-country nationals or stateless persons who have not yet filed an asylum application. Eurodac would no longer be only an "asylum database" but also serve other immigration purposes because it would be possible to check fingerprints of apprehended irregular immigrants. Moreover, in the future Eurodac would also store photos, names, dates of birth, nationalities and identity documents so that a person could be identified without contacting the country which entered the data. There are also plans to reduce the minimum age for taking fingerprints from 14 to six years.

12.2.2 Data retention 2.0

After the Federal Constitutional Court (decision of 2 March 2010 - 1 BvR 256/08) and later the European Court of Justice (decision of 8 April 2016 - C-293/12 and C-594/12) had declared the legislation on preventive retention of telecommunications traffic data unlawful at national and European level, in spring 2015 regulators were once again in the starting blocks.

Unfortunately, they did not set out for a middle- or long-distance race, where they could deliberately choose an appropriate pace, but rather for a 100-metre dash. In May 2015, the Federal Ministry of Justice and Consumer Protection (BMJV) presented a bill to reintroduce preventive data retention. In violation of the Joint Rules of Procedure of the Federal Ministries, the bill was adopted by the Cabinet within only seven days with very little time to comment and no interministerial meeting. This is unacceptable for a far-reaching legislative procedure which results in massive infringements upon the citizens' fundamental rights.
However, not only the procedure was questionable. While the provisions have been given a new name – Act to introduce a storage requirement and maximum retention periods for traffic data (*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*) – many of the legal pitfalls of previous acts persist. Even though under the new act infringements are less severe than under the act struck down by the Federal Constitutional Court, e.g. because of shorter retention periods and the exception for e-mails, and the requirements of the court regarding data security have been taken into account, there are still major doubts whether the new provisions comply with the Basic Law (cf. Box a on no. 12.2.2).

For a full list of the shortcomings, please refer to the detailed comments that I submitted to the German Bundestag during the legislative procedure (available at: www.datenschutz.bund.de). In the following, I will address two of the arguments for my assessment: Irrespective of its more "restrictive" nature, the current version of preventive data retention, too, is a fundamental rights infringement of exceptional gravity and scale. Both the Federal Constitutional Court and the European Court of Justice (ECJ) clarified that such measures must be subject to strict requirements so

that their impact can be appropriately assessed. Although regulators obviously made some effort, the act does not live up to the standards set by the supreme courts.

The provisions on the surveillance of Internet use ignore the requirement of the Federal Constitutional Court to refrain from suspicionless data retention which – together with otherwise collected data – could help retrace almost all activities of citizens (researchers call the court's requirement to consider "the totality of the various data pools already in existence" *Überwachungsgesamtrechnung* or surveillance footprint evaluation). However, government authorities are increasingly able to do this because in recent years, they have been given more and more powers, in particular to record and analyse IP addresses.

The collected IP addresses can help them obtain detailed information about the content used on the Internet. Together with the IP data collected in the framework of preventive data retention, data collected with telemedia services can generally be attributed to individual users. This way, authorities can monitor the users' browsing habits to a considerable extent over several weeks.

Moreover, the act ignores the requirements of the aforementioned ECJ ruling stating that data retention must be restricted to persons who are in any way involved in a serious crime or whose retained data may help prevent, detect or investigate serious crimes for other reasons. Therefore, the act disproportionately interferes with the right to respect for private and family life and the right to protect personal data granted under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter).

In a recent ruling on Swedish and British data retention acts, the ECJ once again clarified that the Charter also applies to national legislation (decision of 21 December 2016 - C-203/15 and C-698/15). In this context, the court unequivocally repeated that a general and indiscriminate retention of all traffic and location data of all telecommunications users is not compatible with European law. The court permits only targeted retention of data that is limited to what is strictly necessary with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, .

Significantly expanding retention obligations, e.g. by including data generated when using e-mail and messaging services, and extending retention periods would expand preventive data retention beyond the provisions of the act revoked by the Federal Constitutional Court in 2010.

Apart from that, I seriously doubt that the current act introducing a retention obligation and a maximum retention period for traffic data meets the strict requirements of the Federal Constitutional Court and the ECJ. However, the final decision on that matter will once again rest with these courts. Given the ECJ's decision on the applicability of the Charter, the court will likely be asked to review the German data retention provisions. Several constitutional complaints have already been filed with the Federal Constitutional Court.

Of course, I will observe the proceedings and monitor the practical implementation of the act by telecommunications companies from a data protection perspective.

Specifications, ordinance, guidelines

The provisions on preventive data retention in the Telecommunications Act (Telekommunikationsgesetz, TKG) not only require a list of specifications but also refer to the Ordinance on Telecommunications Interception (Telekommunikationsüberwachungsverordnung, TKÜV) and the Technical Guidelines for the implementation of legal telecommunications interception measures and the disclosure of information (Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften, TR TKÜV). These provisions, too, must be revised.

Telecommunications providers must ensure a particularly high standard of data security and data quality for preventive data retention. This is another request of the Federal Constitutional Court reflected in the act. The Telecommunications Act is not very specific about how this should be done and requires that details should be provided in specifications pursuant to Section 113f of the TKG. Together with the Federal Office for Information Security (BSI) and my authority, the Federal Network

Agency (BNetzA) developed these specifications. If the parties subject to preventive data retention obligations meet these requirements, a sufficient level of security can be assumed.

Traffic data is to be stored in a central storage infrastructure that uses firewall systems for physical and logical protection from attacks (cf. Box b on no. 12.2.2).

In addition to defining the basic architecture, many technical and organizational details had to be clarified when preparing the specifications. This was not always easy because a high security level was needed which, however, could be implemented in practice with reasonable effort.

For example, one requirement was to ensure that traffic data subject to data retention are irreversibly deleted after the retention period has expired. Modern storage media (magnetic hard drives and SSDs) can disable bad sectors, i.e. they cannot be read by the operating system. This means that data can no longer be reliably deleted. Therefore, day keys are to be used for encrypted storage of “retained data”. If the day key is reliably deleted after the regular retention period has expired, the encrypted data are also considered deleted. This requires reliable key management. Although the encrypted data must still actually be deleted, this no longer requires special efforts.

Another special challenge is to make the query system secure. Section 113c (3) of the TKG refers to the Ordinance concerning the Technical and Organizational Implementation of Measures for the Interception of Telecommunications (TKÜV) and the Technical Guidelines for the implementation of legal telecommunications interception measures and the disclosure of information (TR TKÜV). Even if this reference was intended to create synergies with existing query systems for other information purposes (e.g. disclosure of corporate inventory and traffic data), it makes developing the specifications more difficult.

Instead of providing for the disclosure of data in the overall framework for the specifications described above, the issue had to be singled out and implemented in the course of revising the TKÜV and the related technical guidelines. It would have

made sense to amend these provisions along with developing the specifications. However, since different bodies are responsible for developing and revising the individual provisions, the specifications had been developed before the ordinance and the technical guidelines were revised. Therefore, the latter were not completed at the time this report went to press. I have seen the initial drafts, and finalization of the provisions before storage becomes mandatory in July 2017 seems likely. Whether transitional solutions will have to be used given the time needed for technical implementation remains to be seen.

The TKÜV includes a new section on the disclosure of traffic data which also includes the provision on logging. No difference is made for traffic data stored and to be stored by companies, i.e. the strict requirements also apply to data used within companies.

Other areas were revised as well. Fortunately, it is no longer planned to send orders by fax. Moreover, information requests may be answered only electronically. Further amendments were made concerning the surveillance of communications between non-German citizens abroad by the Federal Intelligence Service, for example (cf. no. 10.2.10.1). The new rules also permit discreet remote maintenance of facilities of the Federal Intelligence Service. So far remote maintenance has not been allowed; now *unauthorized* remote maintenance is forbidden.

In addition to the technical implementation of surveillance measures, the TR TKÜV also provides for measures to implement the disclosure and transmission of information. Large providers are subject to the ETSI-ESB. (ETSI is the European Telecommunications Standards Institute which created the underlying European standard; ESB stands for *Elektronische Schnittstelle Behörden*, specifications for the electronic interface of authorities to request information and connection data and for telecommunications surveillance and detection.) In particular the requirements for data retention have been added to the TR TKÜV. Small providers with fewer than 100,000 users may also use the simplified “E-Mail-ESB” so that – announced – orders can be received and answered via encrypted e-mail.

Whether these new rules actually meet the high data protection and data security requirements can be assessed only when their final version is available. The TKG covers any processing of data stored by telecommunications providers, i.e. collection, storage and the processes to disclose information. Therefore, the specifications of the ordinance and the guidelines must be considered as a coherent whole. This means that the task of specifying the general provisions of the TKG, which I share with the BNetzA and the BSI, will be completed only when this interrelated framework has been completed and has entered into force. Practical implementation by the companies will show whether the provisions can be applied consistently, which I hope. I will pay various telecommunications providers informational and inspection visits to see how it works.

Box a on no. 12.2.2

Key requirements of data retention 2.0 at a glance

Obliged parties (*Section 113a TKG*)

- Providers of publicly accessible telecommunications services (except hotels, coffee shops, etc.)

Data to be stored (*Section 113b TKG*)

- *for telephone calls, SMS and MMS*:
  - the numbers or identifiers of the telephone lines involved in the connection/transmission
  - date and time of the start and end of the connection/transmission
  - for mobile services additionally the SIM card number (IMSI), the identifier of the device used (EMEI) and the radio cell where the connection started
  - for IP telephony additionally the IP addresses of the participating telephone lines and the assigned user ID

- *for Internet use*:
  - IP address

- line and user ID
- date and time of the start and end of the Internet use from an IP address
- for mobile Internet use additionally the radio cell where the connection started

Retention periods (*Section 113b TKG*)

- location data (radio cells) – four weeks
- any other data – ten weeks

Bodies authorized to request data (*Section 113c TKG*)

- federal and state law enforcement authorities
- state threat prevention authorities

Other

- The data may be used only to prosecute serious crimes as specified in the Code of Criminal Procedure (*Strafprozessordnung*, StPO) or to avert a concrete threat to life, limb or freedom of a person or to the existence of the Federation or a federal state; the only exception is attributing an IP address to the owner of a connection (*Section 113c TKG*).

- The data must be protected from misuse by state-of-the-art means (e.g. secure encryption, storage disconnected from the Internet, four-eyes principle for access) (*Section 113d TKG*).

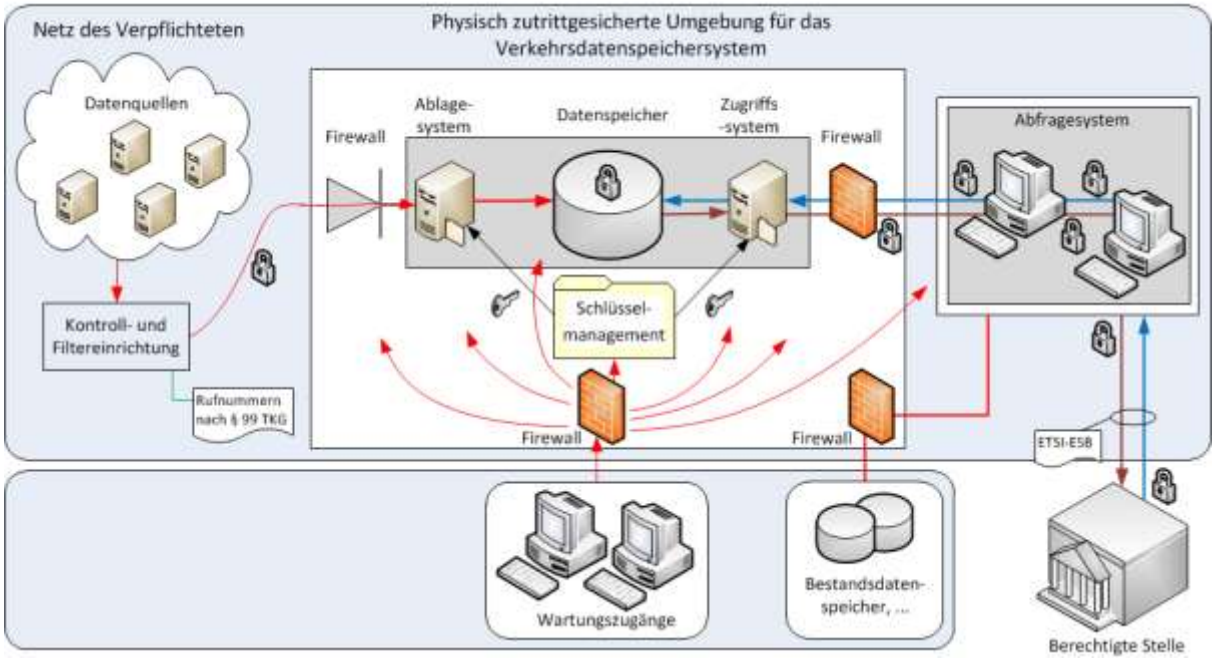
- Access to the data must be recorded (*Section 113e TKG*).

- Together with my authority and the BSI, the BNetzA develops specifications (*Section 113f TKG*).

- The storage obligation starts on 1 July 2017.

Box b on no. 12.2.2

Example for the implementation of the basic architecture



Kasten b zu Nr. 12.2.2

Netz des Verpflichteten	Network of the obliged party
Datenquellen	Data sources
Kontroll- und Filtereinrichtung	Control and filter mechanism
Rufnummern nach § 99 TKG	Telephone numbers under Section 99 TKG
Physisch zutrittgesicherte Umgebung für das Verkehrsdatenspeichersystem	Physically secure environment for the traffic data storage system
Firewall	Firewall
Abfragesystem	Query system
Datenspeicher	Data storage
Zugriffssystem	Access system
Firewall	Firewall
Schlüsselmanagement	Key management
Firewall	Firewall
Firewall	Firewall
Wartungszugänge	Access for maintenance
Bestandsdatenspeicher, ...	Subscriber data memory, ...
Abfragesystem	Query system
ETSI-ESB	ETSI-ESB
Berechtigte Stelle	Authorized body

Kasten, Seite 39:

Fiktives Beispiel: Kontrolle einer Person (X) in der ATD	Scenario: Reviewing a person (X) in the counter-terrorism database (ATD)
drei Sicherheitsbehörden des Bundes haben Daten zu X in der ATD gespeichert; diese stammen aus den jeweiligen ATD-Quelldateien dieser Behörden	three federal security authorities stored data on X in the ATD; these data come from the individual ATD source databases of these authorities

Inhalt der ATD zu X	Data on X in the ATD
Sicherheitsbehörde 1: Vorname, Name, Wohnort, bes. Fähigkeiten, Gefährder	Security authority 1: first name, last name, address, special skills, potential perpetrator
Sicherheitsbehörde 2: Name, bes. Merkmale, Kontaktperson	Security authority 2: name, special characteristics, contact person
Sicherheitsbehörde 3: Name, Wohnort, bes. Fähigkeiten, Gefährder	Security authority 3: name, address, special skills, potential perpetrator

Sicherheitsbehörde 1 (Nachrichtendienst)	Security authority 1 (intelligence service)
Vorhandene Daten zu X:	Data available on X:
ATD-Quelldatei	ATD source database
Person X	Person X
Vor- u. Nachname	first and last name
Wohnort	address
bes. Fähigkeiten	special skills
Gefährder	potential perpetrator
sonstige Erkenntnisse (die nur in dieser Quelldatei, nicht aber in	other findings (that may be stored only in this source database but

der ATD gespeichert werden dürfen).	not in the ATD)
sowie	and
andere Dateien/Akten mit Daten des X	other files with data of X
(aktuelle) Maßnahmen der Sicherheitsbehörde 1 gegenüber X: Observation, Telekommunikationsüberwachung nach dem G10-Gesetz	(current) measures of security authority 1 related to X: observation, telecommunications surveillance under the G10 Act

Sicherheitsbehörde 2 (Nachrichtendienst)	Security authority 2 (intelligence service)
Vorhandene Daten zu X:	Data available on X:
ATD-Quelldatei	ATD source database
Person X	Person X
Nachname	last name
bes. Merkmale	special characteristics
Kontaktperson	contact person
sonstige Erkenntnisse (die nur in dieser Quelldatei, nicht aber in der ATD gespeichert werden dürfen).	other findings (that may be stored only in this source database but not in the ATD)
sowie	and
andere Dateien/Akten mit Daten des X	other files with data of X
(aktuelle) Maßnahmen der Sicherheitsbehörde 2 gegenüber X: GPS-Überwachung	(current) measures of security authority 2 related to X: GPS surveillance

Sicherheitsbehörde 3 (Polizeibehörde)	Security authority 3 (police)
Vorhandene Daten zu X:	Data available on X:
ATD-Quelldatei	ATD source database

Person X	Person X
Nachname	last name
Wohnort	address
bes. Fähigkeiten	special skills
Gefährder	potential perpetrator
sonstige Erkenntnisse (die nur in dieser Quelldatei, nicht aber in der ATD gespeichert werden dürfen).	other findings (that may be stored only in this source database but not in the ATD)
sowie	and
andere Dateien/Akten mit Daten des X	other files with data of X
(aktuelle) Maßnahmen der Sicherheitsbehörde 3 gegenüber X: Wohnraumüberwachung und Telekommunikationsüberwachung	(current) measures of security authority 2 related to X: surveillance of homes and telecommunications surveillance

Kasten b zu Nr. 1.3, Seite 40:

Erläuterungen zum fiktiven Beispiel: Kontrolle einer Person (X) in der ATD	Explanation of the scenario: Reviewing a person (X) in the counter-terrorism database (ATD)
drei Sicherheitsbehörden des Bundes haben Daten zu X in der ATD gespeichert	three federal security authorities stored data on X in the ATD

(Verfassungs-)rechtlich vorgegebener Ablauf/Umfang der Kontrolle:	Procedure/scope of the check under (constitutional) law:
1. Prüfung der ATD-Speicherung der Sicherheitsbehörde 1 wie folgt:	1. Reviewing ATD storage by security authority 1 as follows:

a) Ist die ATD-Speicherung nach den Vorgaben des ATDG zulässig.	a) Does ATD storage meet the requirements of the ATD Act?
b) Sind die Daten aktuell und identisch in der (den) ATD-Quelldatei(en) gespeichert.	b) Are the data up to date and stored identically in the ATD source database(s)?
c) Ist die Speicherung in der Quelldatei rechtlich zulässig (entspricht sie insbesondere den Vorgaben der einschlägigen Dateianordnung; falls nicht, ist die ATD-Speicherung unzulässig).	c) Is storage in the source database lawful (in particular, does it meet the requirements of the pertinent file order; if not, ATD storage is not permitted)?
d) Wurden die in der Quelldatei gespeicherten Daten rechtlich zulässig erhoben (falls nicht, ist die ATD-Speicherung unzulässig).	d) Were the data stored in the source database collected lawfully (if not, ATD storage is not permitted)?
e) Liegen verfassungsrechtlich unzulässige „additive Grundrechtseingriffe“ zu Lasten des X durch diese Sicherheitsbehörde vor, d.h. Ermittlung und Bewertung aller bei dieser Sicherheitsbehörde zu X vorhandenen Daten / Maßnahmen (Vorgabe des Bundesverfassungsgerichts).	e) Did this security authority repeatedly infringe upon the fundamental rights of X (“additive infringements”) in violation of the Constitution? I.e. investigating and assessing all data / measures of this security authority relating to X (requirement of the Federal Constitutional Court).

2. Prüfung der ATD-Speicherung der Sicherheitsbehörde 2 wie folgt:	2. Reviewing ATD storage of security authority 2 as follows:
Siehe oben 1 a) - e).	See above 1 a) - e).

3. Prüfung der ATD-Speicherung der Sicherheitsbehörde 3 wie folgt:	3. Reviewing ATD storage of security authority 3 as follows:
Siehe oben 1 a) - e).	See above 1 a) - e).

4. Prüfung aller Daten/Maßnahmen aller Sicherheitsbehörden	4. Reviewing all data/measures of all security authorities
Liegen unzulässige „additive Grundrechtseingriffe“ zu Lasten des X durch das Zusammenwirken der Maßnahmen aller Behörden vor.	Did the measures of all authorities together cause inadmissible “additive infringements of fundamental rights” to the detriment of X?
Notwendig ist demnach eine Zusammenschau und Bewertung der zu X bei allen Behörden vorhandenen Daten / Maßnahmen (Vorgabe des Bundesverfassungsgerichts).	It is therefore necessary to review and assess the data / measures of all authorities relating to X (requirement of the Federal Constitutional Court).
Konsequenz: Eine bzw. einzelne Maßnahmen könnten - rechtlich isoliert betrachtet - verfassungsrechtlich zulässig sein und sich erst in dieser Zusammenschau als verfassungswidrig erweisen.	Consequence: One or individual measure(s) could - when viewed in isolation - be permitted by the Constitution and turn out to be unconstitutional only when assessed in the context of other measures.
Die Sicherheitsbehörden sind verpflichtet, dies durch eine entsprechende Kooperation/Abstimmung auszuschließen (Vorgabe des Bundesverfassungsgerichts).	Security authorities are obliged to prevent this through appropriate cooperation/coordination (requirement of the Federal Constitutional Court).

Kasten a zu 10.2.11.5

IT-Sicherheit nach dem Grundschutz	IT security according to the baseline security model
Niedrig/mittel	Low/medium
Hoch/sehr hoch	High/very high
Bedrohungs- und Risikoanalyse	Threat and risk analysis
Grundschutz nach dem Grundschutzhandbuch	Baseline security according to the Baseline Protection Manual
Nach dem IT-Sicherheitshandbuch oder anderen Verfahren	According to the IT Security Manual or other procedures
BSI-Grundschutzhandbuch	BSI Baseline Protection Manual

Kasten b zu 10.2.11.5

IT-Sicherheit, Datenschutz und Datensicherheit nach dem Grundschutz und Standard-Datenschutzmodell	IT security, data protection and data security according to the baseline security model and the standard data protection model
Grundschutzhandbuch	Baseline Protection Manual
SDM-Handbuch	SDM Manual
Anwenden des Grundschutzes	Applying baseline security model
Anwenden des Standard-Datenschutzmodells	Applying the standard data protection model
IT-Sicherheit, Datenschutz, Datensicherheit gewährleisten	Ensuring IT security, data protection and data security