future in a specific Ethic Committee for the application of AI in the defence area. This should also affect the private partners and the researchers involved in such AI projects.

Mainly, the ANSSI with its cyber defence centre can support the victims of industrial espionage. DFIR ORC is for instance an open-source modular framework to collect forensic artefacts on machines running a Microsoft Windows operating system created in 2011 to address operational needs of incident responders. The ANSSI also provides to the actors a list of recommended software, they might use for protection against industrial espionage and other confidentiality breaches. Finally, the ANSSI develops research projects on its own or with partners and is equipped with a Scientific Committee. It might be able to elaborate technical tools required.

11 Germany

Harald Zwingelberg (ULD)

11.1 Informed consent

11.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
General Data Protection Regulation (GDPR)	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679	EU regulation, hard law	Harmonized European data protection law
Federal Data Protection Act (Bundesdatenschutz-gesetz, BDSG)	https://www.gesetze-im-internet.de/englisch_bdsg/	hard Law	
State Data Protection Acts (Landesdatenschutz-gesetze, LDSG[83])	Overview page with links: https://dswiki.tu-ilmenau.de/liste_der_landesdatenschutzgesetze	hard Law	
Gesetz zur Regelung des Datenschutzes und des Schutzes der	https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_	hard law as of December 1st 2021	Summarizing data protection related laws currently spread in

[83] Links to the state data protection acts have been collected here including links to the central parliamentary documents motivating the law and usually containing some core considerations on each of the articles. https://dswiki.tu-ilmenau.de/liste_der_landesdatenschutzgesetze.

Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG)	BGBl&start=//*[@attr_id=%27bgbl121s1982.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1982.pdf%27%5D__1628844177100		spate acts on telecommunication and telemedia.
Telemediengesetz, TMG	https://www.gesetze-im-internet.de/tmg/	hard law	Telemedia Act governing telemedia See Sections 11 et seq. TMG on data protection
Telekommunikations gesetz (TKG)	https://www.gesetze-im-internet.de/tkg_2004/	hard law	Telecommunications Act See Sections 91 et seq. TKG for data protection and Sections 108 et seq. TKGon public security / cybersecurity

Main regulatory tools addressing data protection and informed consent in Germany

As a European regulation, the GDPR is directly applicable in Germany. Where the GDPR contains opening clauses that allow Member States to modify or amend the harmonized provisions in order to cater for specific aspects of national law, the German data protection laws typically implement this.

The regulatory Framework in Germany reflects the federal structure of Germany laid down in the German Constitution (Grundgesetz, GG); all legislative powers not assigned to the federal government are assigned to the 16 federal states (German: Bundesländer). Due to this federal structure, data protection legislation exists at both, the level of federal states and the federal level. Likewise, data protection authorities (DPAs) have been established at both these levels (see below for details).

The federal data protection act (Bundesdatenschutzgesetz, BDSG) governs federal public entities and the private sector nationwide. According to section 1 paragraph 5 BDSG, where the GDPR holds applicable provisions, the European regulation prevails. The following considerations will mainly focus on the federal law with some pointers to selected laws of the federal states.

Beyond the general regulatory framework for data protection set by the GDPR and the German data protection acts, specific provisions are contained in sector-specific laws at federal and state level. To align these sector-specific laws with the provisions and terminology of the GDPR and the BDSG, the federal legislator passed an omnibus-act that

amends and changes data-protection-related norms in more than 150 individual laws.[84] Within their scope of application, these specific laws usually supersede more generic laws.

With regard to PANELFIT's focus on ICT-research and innovation, it is important to note that the majority of universities and research institutions in Germany are public entities and are therefore subject to the data protection acts of the federal states (Landesdatenschutzgesetz, abbreviated as LDSG). However, the sixteen data protection acts of the federal states have all been adapted when the GDPR went into effect and thus differ only in smaller details regarding data processing for research purposes. Furthermore, they get supplemented by specific University and College Acts (Hochschulgesetze). Medical research done at hospitals may be subject to additional requirements in the Hospital Acts (Krankenhausgestze) of the respective federal states. For example, these Hospital Acts foresee that the consent for data processing in this area usually requires a written form.

(i) The GDPR does not apply to purely personal or household activity. Is there any provision under national law for the protection of these data categories?

There are no legislative rules in place on how the processing of personal data falling under this exception must be handled. The common understanding in German legal literature is that the household exemption is seen as an exception from the general rule and requires a strict and narrow interpretation.

(ii) The GDPR does not apply to national security. Is there any national regulation covering this topic (in terms of data protection issues)?

The Directive 2016/680 of 27 April 2016 "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"[85] has been enacted into German national law. To this effect, an omnibus act[86] was passed re-structuring the federal data protection act (BDSG) and a series of other federal laws. The BDSG now contains generic provisions for federal public entities who operate in the area of national security. Furthermore, several (existing) specific laws for agencies concerned with national security have been amended to implement Directive 2016/680. These agencies include the following:

Bundesamt für Verfassungsschutz, BfV, (Federal Office for the Protection of the Constitution)[87]

Bundesamt für Sicherheit in der Informationstechnik, BSI, (Federal Office for Information Security)[88]

[84] Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl119s1626.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl119s1626.pdf%27%5D__1627645119795.

[85] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680.

[86] "Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680. Published in the official journal: Bundesgesetzblatt 2017, pages 2097 et seq. https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1627628814209.

[87] Bundesverfassungsschutzgesetz, https://www.gesetze-im-internet.de/bverfschg/.

[88] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, see in particular §§ 3a GSI-G et seq. At: https://www.gesetze-im-internet.de/bsig_2009/.

Bundesamt für den Militärischen Abschirmdienst, MAD, (Military Counterintelligence Service)[89]

Bundesnachrichtendienst (Foreign Intelligence Service) [90]

In parallel the legislators of the federal states passed acts amending the laws on their respective Landesämter für Verfassungsschutz, LfV, (offices for the protection of the constitution in the federal states)[91]

In addition, data processing by police forces are governed by specific legislation that is part of so called "police laws" at both, federal and state level.

Information regarding Data Protection Authorities in Germany

Name of Authority	Link	Is this an independent body?	Number of employees	Level of activity	Response to requirements, questions, etc. made by the public
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	https://www.bfdi.bund.de/EN/Home/home_node.html	yes	~230	Takes active role within its area of responsibility	See note below
Landesbeauftragte(r) für den Datenschutz	For a list see: https://www.bfdi.bund.de/DE/Home/home_node.html.	Yes	Varying by state and depending on the state's population and number of enterprises	The commissioners take an active role within their respective area of responsibility	See note below

Data protection authorities (DPAs) have been established at both the federal and state levels.[92]

[89] Gesetz über den militärischen Abschirmdienst, https://www.gesetze-im-internet.de/madg/.
[90] Gesetz über den Bundesnachrichtendienst, https://www.gesetze-im-internet.de/bndg/.
[91] Specific legal regulations exist as part of the legislation of the federal states in the respective "Landesverfassungsschutzgesetez".
[92] For a list of the data protection commissioners of the states see: https://www.bfdi.bund.de/DE/Home/home_node.html.

In the system of data protection authorities in Germany, each authority has full competence within their territorial and subject matter jurisdiction. All DPAs have subject matter competence for public administrations located in their jurisdiction. For all private entities, encompassing both, natural persons and corporations, the competence of the state-level DPAs depends on the territorial residence of the controller. An exception to this rule is made for telecommunication companies which fall in the jurisdiction of the Federal Data Protection Commissioner. The Federal Data Protection Commissioner is also competent for all federal-level public bodies.

The authorities cooperate with the objective to harmonize their interpretation of the data protection legislation in Germany. In particular, the "Conference of the Independent Data Protection Authorities of the Bund and the Länder" ("Datenschutzkonferenz", DSK)[93] issues resolutions, guidelines, and positions papers to harmonize the application of data protection legislation in Germany. Together with opinions, guidelines and decisions by the European Data Protection Board (EDPB), these publications are highly relevant in the interpretation and understanding of data protection legislation in Germany.

Note on the activity of data protection authorities (DPAs) in Germany: Request of data subjects in a specific case, have a high priority in all German DPAs. Response times may vary as the workload for the DPAs has highly increased as the GDPR massively raised public awareness for data protection related issues. The DPAs cooperate as part of the Datenschutzkonferenz. with information in form of resolutions, guidelines and white papers for data subjects and data controllers alike. The individual DPAs also provide information on their websites covering frequent questions.

(iii) Does your national legislation introduce a specific definition of "data processing for research purposes"? Does your national legislation define "research in public interest", e.g. referring to Ministerial lists of expected research, etc.?

The Federal Data Protection Act defines neither "research" nor "research in the public interest". Research is therefore understood[94] as it is defined in Article 13 of the Charter of Fundamental Rights of the European Union[95] and in the corresponding German fundamental right of Article 5 Paragraph 3 in the German constitution (Grundgesetz).

The derogations from the GDPR (as permitted in Article 89 GDPR for scientific or historical research purposes) are laid down in section 27 BDSG without addressing the definition of "*research"*. In the relevant German legal literature, privately funded research is considered to be research under the condition that commercial purposes must not overlap with the scientific research interests and that the commercial interests cannot influence the cognition and research process.[96]

(iv) Does your national legislation implement Article 89 of the GDPR, introducing in particular some specific safeguards to adopt in case of data processing for research purposes?

Section 27 BDSG implements Article 89 GDPR and refers to Section 22 Paragraph 2 BDSG for the measures. Parallel provisions are part of the Data Protection Acts of the federal states.

[93] https://www.datenschutzkonferenz-online.de/.
[94] Weichert, "Die Forschungsprivilegierung in der DS-GVO" in ZD 2020, p 19.
[95] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN.
[96] Buchner/Tinnfeld in Kühling/Buchner DSGVO, § 27 BDSG para. 5 and Art. 89 DSGVO para. 12 et seq.; Weichert, „Die Forschungsprivilegierung in der DS-GVO", in ZD 2020, p. 29-20.

(v) Does your national legislation provide specific cases and safeguards for processing sensitive data beyond Article 9 of the GDPR? Which cases? Which safeguards?

The German Federal Data Protection Act (Bundesdatenschutz-gesetz, BDSG) foresees several measures that safeguard special categories of data.

Section 22 BDSG provides a list of generic measures and requirements for the processing of special categories of personal data. These apply to the cases where Article 9(4) allows Member State law to maintain or introduce further conditions, i.e., the processing of genetic data, biometric data or data concerning health. In particular, Section 22, Paragraph 2 BDSG reads as follows [translated from German]:[97]

> "In the cases of subsection 1 [list of legal grounds for processing special categories of data], appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following
> 1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;
> 2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
> 3. measures to increase awareness of staff involved in processing operations;
> 4. designation of a data protection officer;
> 5. restrictions on access to personal data within the controller and by processors;
> 6. the pseudonymization of personal data;
> 7. the encryption of personal data;
> 8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
> 9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
> 10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes.

Widely similar lists with measures are included in the Data Protection Acts of the federal states.

In the context of the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the national implementations under the opening clause in Article 89 contain some details regarding special categories of data. In particular, Section 27 BDSG allows for the processing of special categories of data for these archiving purposes without a specific consent by the data subjects. For this, a weighing-test between the interests is necessary. In particular, the controller's interests must considerably (German: "erheblich") outweigh the interest of the data subjects.

[97] Translations provided by the Language Service of the Federal Ministry of the Interior. https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0175.

Section 27 also refers to the list of measures of Section 22 Paragraph 2 BDSG (see above). Accordingly, special categories of data must be anonymized as soon as the purposes permit it. Where anonymization is not possible, information that allows the identification of data subjects must be pseudonymized (see Paragraph 3 of Section 22 BDSG)

According to Section 48 BDSG, the processing of special categories of data for purposes in accordance with Article 1 (1) of Directive (EU) 2016/680 must be strictly necessary and appropriate safeguards must be taken.

Further specific legislation applicable to special categories of data exist e.g. for hospitals. These are widely spread in the Hospital Acts of the federal states or, where a church, the military or the police operates a hospitals, also in the respective data protection laws and acts of the particular entity. An overview of further specific rules for special categories of data is provided by Weichert in Kühling/Bucher.[98]

(vi) Do you have a national (or some regional) Code(s) of Conducts or national Code of Ethics for data processing in research? Could you please summarize the content of such codes (specifying scope, suggested measures to protect individuals, prohibitions, exemptions, etc.)?

Please refer to the section "9.11.5 Governance" at the end of this country report for a selective overview of ethic boards based on national legislation as well as the applicable laws and regulations, e.g. in pharmaceutical research.

Sector-specific codes of conduct have been established by initiative of the involved institutions such as universities.

(vii) Does your national legislation give specific definitions of data processing for "statistical purposes"? Are there specific rules that apply to such data processing?

There is no further definition of statistical purposes in the national legislative texts. The legal literature refers to recital 162 GDPR for this purpose. Based on the understanding of the recital, only processing that results in aggregated (usually not personal) data is considered to be processing for statistical purposes. This excludes inter alia scoring and other big-data-based processing of personal data.

Whether commercial statistics fall under the privileges granted by Article 89 GDPR remains an open question in the legal literature. The wording "in the public interest" in Article 89 GDPR insofar only relates to archiving purposes and not to statistics. Due to the nature of the privileges granted and to the resulting limitations of the fundamental rights and freedoms, the literature argues that the privilege may only apply where the processing is justified by overarching public interests. This would exclude statistical processing where commercial interests overlap with the statistical purposes, e.g. where processing takes place for direct marketing, market analysis or risk assessments.

(viii) Are there any other references to data processing for research purposes in your national legislation? (e.g. duties to have a DPO, duties to perform a DPIA, duty to collect consent, etc.)

All public entities must appoint a data protection officer. As the vast majority of universities, colleges, and research institutes are public entities, this applies to most them. As for private

[98] Weichert in Kühling/Buchner, 3rd ed., 2020, Article 0 DS-GVO Number 168 et seq., https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FKueBuchnerKoDSGVO_3%2Fcont%2FKueBuchnerKoDSGVO%2Ehtm.

research institutions, it is also highly likely that also they must appoint a data protection officer. This is since either their core activities involve the processing on a large scale of special categories of data (e.g. in the field of medial or psychological research) or since their size exceeds 20 employees involved in the processing of personal data (see Article 37 (1) (b) GDPR and Section 38 Paragraph 1 BDSG).

As for data protection impact assessments, the German data protection authorities published non-exhaustive lists of processing activities that require a DPIA.[99] These lists specifically refer to research that is related to genetic databases for genealogical research and the anonymization of data for research purposes.

11.1.2 Rights of data subjects and data processing

(i) Are there any special requirements regarding informed consent at the national level?

No specialties known that constitute a relevant deviation from the GDPR-ruleset.

(ii) Are there any special requirements regarding data processing at the national level?

Special requirements related to consent in general that constitute notable deviation from the GDPR are not known.

A sector specific deviation exists for working relationships in Section 26 Paragraph 2 BDSG.[100] According to this rule, special caution is necessary when evaluating, whether consent has been given freely by employees. For this all circumstances must be considered under which the consent has been given in the light that the typical power asymmetry between employee and employer. Under the old national law it was a broadly assumed that free consent is usually not possible where such power asymmetries between data controller and data subject exist. Beyond employee and employer relationships this line of thought applied to landlord and tenants as well as the provision of vital services such as the delivery of water and electricity. While this is not part of the written law understanding the consideration is a useful background-information. Where such power asymmetries exist, this will likely influence the interpretation and understanding of the law by German legal practitioners and may influence decisions e.g. where the law asks for a balancing of interest test.

(iii) Are there any special requirements to exercise data subject's rights (right of access, correction, deletion of personal data)?

Data subject rights are governed by the harmonized ruleset in Article 12 et seq. GDPR. There are no additional or "special" national requirements known that data subjects have to fulfil to make use of their data subject's rights that deviate from the GDPR. This will likely be considered to be in conflict with the European law, too.

The national implementation of the limitations provided for in the opening clause Article 89 (2) GDPR for scientific and historic research as well as statistical purposes in opening clause see Section 27 Paragraph BDSG and similar norms in the Data Protection Acts of the federal states.

In some areas of law specific rights stemming from parallel norms supplement the data protection legislation. E.g. for medical doctors section 630a German Civil Code

[99] E.g., refer here for the list published for the state of Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/dsgvo/2018_10_17_DPIAList1_1_Germany_EN.pdf.
[100] Section 26 BDSG is based on the opening clause in Article 88 GDPR.

(Bürgerliches Gesetzbuch, BGB) the treatment contract between physician and patient is defined. The BGB provides some detailed rules for keeping medical records by doctors and for obtaining copies of such records by the patient. In addition physicians (but also attorneys, tax consultants and several other specific occupations) are mandatory members in a professional chamber with own rulesets, enforced by the chamber containing parallel requirements about keeping medical/case/tax records and providing information or copies thereof to the patients/clients/customers. These rules do not limit any of the data subject's rights granted by the GDPR but rather complement them. The enforcement resides accordingly with the customer reaching out to the competent courts where the legal basis is civil law, or chambers and specific professional courts in case of professional law.

In the domain of national security, cybersecurity and policing the rights to access and correction and deletion may be limited for purposes of national security in accordance with directive (EU) 2016/680.

11.1.3 Minors, sensitive data and other additional categories of data

(i) Are there additional rules beyond the ones enforced by the GDPR for processing special categories of personal data (e.g. sensitive data or data of legal persons/entities)?

The list of special categories of data in article 9 (1) GDPR is considered exhaustive.[101] German society and the legal tradition consider other types of information as particularly sensitive, too including e.g. financial data or information on social contacts. While it is clear that Article 9 GDPR is not applicable here the specific quality of such may likely find its realization otherwise, e.g. when weighing legitimate interests against the interests of affected data subjects or as factor for the severity of risks and freedoms when determining the appropriate technical and organizational measures for Articles 25 and 32 GDPR.

For Telemedia personal data collected from minors e.g. for purposes of age verification and other means, must not be used for commercial purposes, see Section 14a TMG.

Section 203 German Criminal Code (Strafgesetzbuch, StGB) contains regulations for professional secrecy for specific professions such as physicians, psychiatrists, attorneys, tax consultants relying on a particularly well protected trust-relationship between patient/client/customer and the professional. For this section the information protected may be broader yet than the understanding of e.g. health data as defined in recital 35 GDPR. E.g. the plain information that a data subject is patient/client must already not be disclosed (German "offenbaren") by the professional or her/his staff. In the field of research involving data processed by one of the listed professions the limitations of the German Criminal Code should be considered, too. However, a valid informed consent can justify a disclosure or secondary use of the information.

The German social security law provides for another sectoral protection of personal data. Data processed by the governmental social security agencies is under a particularly strict protection. General provisions on the protection of these data are laid down in Sections 67 et. seq. Social Security Act 10 (Sozialgesetzbuch, SGB X) and yet more specific regulations are in the respective acts for e.g. welfare (SGB II), public health insurance (SGB V) or public pension insurance (SGV VI). This specific protection of data processed by social security agencies is not limited to personal data and the protection of natural persons. It rather explicitly extends also to other types of data and information related to legal persons, e.g.

[101] Kuner/Bygrave/Docksey, art. 9 section (C) (1).

companies that must provide extensive information about their workforce and wage structure to pension and health insurances. These rules apply directly only to the social security agencies itself and not to the providers of social services. So doctors and clinics providing health services, social workers or the youth care institutions they work for are not addressees of these norms. However, those persons will most likely work as or on behalf of a professional where Section 203 StGB applies.

(ii) Are there any special rules when processing personal data of children? At what age can a minor provide consent according to your regulation?

Germany did not make use of the clause in Article 8 (1) GDPR for a lower age for consent regarding information society services. Therefore minors must either be 16 years of age or have a consent by the holder of parental responsibility.

For other purposes than services of the information society consent requires sufficient maturity in the sense, that the minor can understand the implications of the consent given. This comprises the general capacity to understand the implications of such types of transactions as well as the implications of the specific case. The maturity is to be evaluated on a case-by-case basis. In addition the consent and the information about the processing provided must be concise, understandable and comprehensible specifically in relation to the age und maturity of the minor asked for consent, see also Art. 12 (1) GDPR.

(iii) Are there other vulnerable individuals identified in your national legislation?

German civil law, as also common in other jurisdictions, requires protection of anyone incapable of making informed decisions on which to base declarations of will. This requirement is not directly reflected in data protection legislation but affects how declarations and actions are interpreted and if these are sufficient for a valid consent. Where persons with mental disabilities or persons placed under legal guardianship are affected, decisions about the necessary maturity will take the limited legal capacity of the data subject into account when assessing the maturity of the data subject; in this case, valid consent may not be possible without involvement of the guardian or parent.[102]

11.1.4 Deceased individuals and personal data

(i) As recital 27 clarifies, the GDPR does not apply to deceased individuals. However, some countries provide people with the right to have all their personal data deleted once they pass away. Some others empower their close relatives to do the same. In some others, these data cannot be used at all without an explicit judicial mandate. What is the situation in your country?

Under German law, deceased persons are provided some protection. The fundamental right to human dignity is understood to entail a core that requires post-mortem protection ("Postmortales Persönlichkeitsrecht"). In particular the reputation of the deceased is protected from being degraded or humiliated.

The surviving relatives have their own rights where their dignity or personality rights are effected. Where the reputation of the deceased can be considered to be a financial asset, these parts of the personality right are inherited and heirs may claim damages and/or obtain an injunction to refrain from further infringements. In 2020, the German Federal Court of

[102] Tinnefeld/Conrad, "Die selbstbestimmte Einwilligung im europäischen Recht", in ZD 2018, p. 393, online: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2018%2Fcont%2Fzd.2018.391.1.htm&pos=12&hlwords=on

Justice upheld a decision that parents in their role as heirs have the right to a functional access to the social media accounts of their deceased minor child.[103]

Also, regulations of professional secrecy do not end with the death of the bearer (see also subsection Minors, sensitive data and other additional categories of data (i) above).

Where personal data is processed for archive purposes, the Archival Laws on federal and state levels regulate the access to information after the death of a person. Details vary but generally, information has to be kept confidential for a minimum of 30 years after a file has been created. Additional time periods are prescribed in other laws. For example, the Federal Archive Act (Bundesarchivgesetz) requires confidentiality for a minimum of 10 years after the death of a person, or if the date of death is unknown, 100 years after the birth of the person or subsidiarily 60 years after the files were created. Similar regulations are found in the archival laws of the federal states, partly stipulating different time periods.

11.1.5 Accountability and Data Protection Impact Assessment

(i) Does your national regulation introduce further provisions related to general accountability? Any particular requirements? Any specific procedures?

The German data protection acts do not explicitly stipulate specific requirements for accountability beyond those in the GDPR.

(ii) Are data protection impact assessments requirements specified by your national regulation? Any particular requirements? Any specific procedures? Any specific reference to data processing in research?

The Conference of the Independent Data Protection Authorities of the Bund and the Länder published a short paper on data protection impact assessment[104] (DPIA) and a list of processing activities that usually require a DPIA.

The German data protection authorities propose the "Standard Data Protection Model" (SDM) as the methodology to conduct DPIAs.[105] It is based on uniform protection goals that capture the essence of the principles stated in Article 5 GDPR and are easy to understand for technical professionals. This methodology supports and guides controllers in the identification of risks and assessment of their severity. It further provides selected modules with measures to mitigate identified risks. The SDM focuses takes an approach centred on fundamental rights of natural persons and freedoms much rather than security based financial and risks of the controller. It thus fosters the identification of risks that may be overseen in a more IT-security-centric assessments. Methodologies other than the SDM that fulfil the requirements of Article 35 GDPR are anyhow permitted.

Concerning the processing of personal data for the purposes of preventing, investigating, detecting, or prosecuting criminal offences, Article 27 of Directive 2016/680/EU has been implemented in section 67 BDSG. It states that the competent authorities are obliged to involve their data protection officers. Furthermore, Section 67 Paragraph 4 BDSG requires some minimum content of the data protection impact assessment.

[103] Bundesgerichtshof, judgement of July 12, 2018, III ZR 183/17, https://openjur.de/u/2110135.html.
[104] DSK, „Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO", https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.
[105] Latest versions of the methodology and modules for the process are published at: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

11.2 Commercialization of data

11.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Data protection legislation, in particular GDPR and federal as well as state data protection acts	See subsection 9.11.4 above	hard law (EU regulation)	See above
EU Regulation on Free Flow of Non-Personal Data (Regulation (EU) 2018/1807)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807	hard law (EU regulation)	
EU Directive on Contracts of Digital Content and Services (Directive (EU) 2019/770)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770	EU directive to be implemented in Member States law	
German Civil Code (Bürgerliches Gesetzbuch, BGB)	https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_BereitstellungdigitalerInhalte.pdf	hard Law, entry into force January 2022	Implementation of the directive on Contracts of Digital Content and Services as of January 2022

Main regulatory tools addressing data commercialization in Germany.

11.2.2 Practice

(i) In practice, does your country allow contracts based on exchange of personal data for services (for instance, to gain access to an app)?

The national data protection legislation does not specifically address this possibility.

The common national interpretation is that Art. 7(4) GDPR applies to this question. The latter is commonly called "prohibition of coupling" (Kopplungsverbot) in Germany and is understood in a narrow manner yet not as a strict prohibition of exchanging personal data in return for goods or services. At EU-level, this concept was discussed by the EDPB in its guidelines on consent[106] under the key word of "conditionality". More insight into the German interpretation can be gained from the guidelines (German: Handreichung) by the Conference of German Data Protection Authorities (DSK) on consent[107] and data processing for advertisement purposes[108].

Effective as of January 2022, Germany will also implement the EU Directive on Contracts of Digital Content and Services in its Civil Code. The implementation neither unconditionally permits nor prohibits the exchange of personal data for services, but it applies the principles of consumer protection as a safeguard for data subjects. In particular, Section 312 (1) and (1a) BGB will render the sections of the BGB on consumer protection applicable to contracts where one party provides personal data that is not strictly required for the performance of the contact.

(ii) Do you know if these practices are routinely performed?

In Germany, these practices are routinely performed and a broad series of services is based on the exchange of personal data in return for services. Examples includes inter alia customer loyalty programs and social networks. Also certain incentive programs rely on personal data. These offer for example benefits as incentives for desirable behaviour by employees or customers of health or vehicle liability insurance. The eligibility for these benefits is then established based on the analysis of data on the relevant behaviour of enrolled persons. In the case of vehicle liability insurance, for example, this typically involves the tracking of driving style.

(iii) Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data?

There are no specific rules on the remuneration of data subjects if profits are made by the controller. Compensation of damages is however foreseen both, by the GDPR (in Article 82) and by German civil law in the context of the infringement of personality rights.

Where data subjects were not informed about profitable processing, there may be a possibility to apply the legal concept of "agency without specific authorisation" (in German „Geschätsführung ohne Auftrag") that is based on the principles of 'negotiorum gestio' in Roman law and thus is likely to be known in other continental law traditions, too. No case law on the use of this concept for remuneration of profitable processing of personal data could be found, however.

[106] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[107] DSK, „Kurzpapier Nr. 20 - Einwilligung nach der DS-GVO", https://www.datenschutzkonferenz-online.de/kurzpapiere.html.
[108] DSK, „Kurzpapier Nr. 3 - Verarbeitung personenbezogener Daten für Werbung, https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

(iv) Do you have any particular national regulation on the secondary use of data?

In the German legal literature it understanding a successful compatibility test Article 6 (4) GDPR does not replace the necessity for a legal ground. Rather a legal ground for the new processing activity must be covered either by one of the legal grounds provided in Article 6 (1) GDPR or sector specific law.

For the secondary use of personal data for archiving purposes in the public interest, scientific or historical research purposes are regulated in Section 27 BDSG and parallel norms of the Data Protection Acts of the federal states.

Secondary use of medical data for research purposes is possible but the data protection related conditions must be met. Legal grounds are spread across the federal and federal states' legislation. Research on basis of secondary use of patient data by hospitals is mainly governed by the Hospital Acts (Krankenhausgestze) and Data Protection Acts of the federal states.[109] These norms usually contain requirements for pseudonymization and anonymization where patient data is used for research purposes.

Further sector specific legal grounds can be found in the social security legislation, e.g. allowing public health insurances the secondary use for statistical and epidemiological research. Cancer-registers have been established in the federal states and on federal level for both epidemiological and clinical research with the patient data. Legal grounds for transmitting, collecting and handling of personal data are thus found in federal states and federal sector specific legislation.[110]

Freedom of Information Acts and Environmental Information Acts have been passed by the federal and most legislators of the federal states. These acts grant rights to access data held by public administrations and also the use for further purposes. However, limitations of the right to access the information namely include personal data and business secrets.

(v) Do you have any specific protection for metadata or non-personal data in your country?

Where metadata is personal data it falls under the protection of the GDPR and the Data Protection Legislation. Specific regulations on the use of metadata exists inter alia for telemedia and telecommunication.

In the Telecommunication Act (Telekommunikationsgesetz, TKG) metadata related to telecommunication activities such as the identifier, phone numbers, location data of mobile devices, start- and end times of connections or the type of telecommunication service. The law refers to this type of data as "Verkehrsdaten", see Section 96 TKG. Telecommunication service providers may only use such data with the data subject's consent for purposes that go beyond the processing necessary to provide the service. Data retention of metatdata and transmitting such information purposes of cybersecurity and criminal prosecution is foreseen in Sections 113 et seq. TKG. The Federal Network Agency has suspended the enforcement

[109] For an overview of the federal state laws see the report written on behalf of the Federal Ministry of Health: Dierks, "Rechtsgutachten - Lösungsvorschläge für ein neues Gesundheitsforschungsdatenschutzrecht in Bund und Ländern", 2019, p. 38 et seq., https://www.bundesgesundheitsministerium.de/service/publikationen/gesundheit/details.html?bmg%5Bpubid%5D=3366.

[110] For a list of legislation on Cancer Registers please refer to: https://de.wikipedia.org/wiki/Krebsregister.

of the data retention requirement for telecommunication providers in 2017 due to an interim measures by a German court.[111]

For telemedia two types of metadata are defined in the German Law on Telemedia (Telemediengesetz, TMG). "Bestandsdaten" are data necessary to establish the contractual relationship, Section 14 TMG. "'Nutzungsdaten" include identifiers information on begin and end of using the service and the type of tele media accessed, see Section 15 TMG. Telemedia service providers may use the latter type of data for optimisation of their services, marketing and market analysis unless the affected person objects.

11.2.3 Nature of Data

(i) How does your country classify data? Is it a product/commodity/good or service? Do you have an additional construct for data?

There does not seem to be any official classification of the legal nature of data in Germany. In the recent years, discussions arose in Germany about this very question, i.e., the legal classification of data. In Germany, there is a consensus among the great majority of experts that data are not material goods and consequently the concepts of property law are not applicable. Much rather, data can be the object of titles and claims under obligation law, either using a contractual basis between the involved parties or as claim for damages where legally granted rights have been infringed. For example, data is closely related to certain rights of different kinds, such as the right to data protection for personal data, copyright for copyrighted works, or the rights laid down in civil law that may lead to claims between persons.

A working group representing the 16 German (state and federal) Ministries of Justice published a report in 2017 that summarizes the according legal situation in Germany. It concludes that it is unnecessary to classify the legal nature of data.[112]

Except for the Sui Generis Right on the protection of databases, do you have a legislation protecting data in your country (e.g. like copyright)? Are you aware of any mechanisms to determine the value of data?

Regarding intellectual property, the German law is harmonized with existing international rules since Germany is member of the EU, the World Trade Organisation, and signatory of a series of treaties in this area. So any data that constitutes intellectual property of some kind, such as works of art, registered designs, or trademarks, are protected under these norms in Germany.

Regarding criminal code, the German law, in Sections 202a, 202b, 202c and 303a of the German Criminal Code (Strafgesetzbuch, StGB), prohibits and punishes certain actions related to data. Note that it is irrelevant whether the concerned data are personal or not. The criminal code addresses in particular the following:

Data espionage, i.e. the access to data that is protected by access control by unauthorized persons (see 202a StGB).

Phishing (see 202b StGB).

[111] Information provided by the Federal Network Agency, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html.

[112] Arbeitsgruppe „Digitaler Neustart", der Konferenz der Justizministerinnen und Justizminister der Länder, „Bericht vom 15. Mai 2017", 2017, https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/index.php.

Unauthorized data manipulation including the deletion, suppression, alteration, or otherwise rendering data unusable (see 202c StGB).

No indication for the existence of a legal or generally accepted mechanism for the determination of the value of data could be found. Court decisions on damages related to the use of data primarily relate to infringement of copyrighted works. Worth mentioning in the context of the value of data is the judgement by the German Federal Court of Justice that has ruled on damages that may be claimed for lost and destroyed data.[113] It has decided that, where the data can be recovered, the damage consists of the costs of this recovery and, where data is irretrievably lost, the damages is equal to the value of the data (without going into the merit of how to determine the latter).

11.3 Security and cybersecurity

11.3.1 General Regulatory Framework

(i) Please describe the main regulatory tools addressing security and cybersecurity in your country following the scheme drawn in the table below. (Please, keep present that the GDPR stipulates that appropriate technical and organisational to protect personal data must be implemented. Is this prevention reflected in your national regulation? Are any particular procedures described in your national regulation? If this is the case, reflect that in the table)

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
GDPR	See above		
BSI-Gesetz (Act on the Federal Office for Information Security, BSI-Act)	In German https://www.gesetze-im-internet.de/bsig_2009/ In English (2009) https://www.gesetze-im-internet.de/englisch_bsig/index.html	hard law	See note 1 below
IT-Sicherheitsgesetz (IT Security Act)	http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf	hard law	See note 2 below
Umsetzungsgesetz zur NIS-Richtlinie	http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1885.pdf	hard law	See note 3 below
Energiewirtschaftsgesetz	http://www.gesetze-im-internet.de/enwg_2005/	hard law	See note 4 below

[113] BGH, judgement of December 9, 2008 - VI ZR 173/07, https://openjur.de/u/72544.html.

(German Energy Act)			
Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV)	https://www.gesetze-im-internet.de/bsi-kritisv/	Material law, issued by the executive	See note 5 below
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code	https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:32018L1972	EU directive	See note 6 below
Telekommunikationsgesetz (TKG)	https://www.gesetze-im-internet.de/tkg_2004/	hard law	See note 7 below
Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommuni	https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/referentenentwurf-zum-telekommunikatiosmodernisierungsgesetz-bgbl.pdf?__blob=publicationFile	hard law	See note 8 below

kationsmoder nisierungsgese tz)			
Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommuni kation und bei Telemedien“ (TTDSG)	https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl121s1982.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1982.pdf%27%5D__1628844177100	hard law as of December 1st 2021	See note 9 below
Telemedienges etz, TMG	https://www.gesetze-im-internet.de/tmg/	hard law	See note 10 below

Notes:
The Act on the Federal Office for Information Security (BSI Act, in German “Gesetz über das Bundesamt für Sicherheit in der Informationstechnik”, short: “BSI-Gesetz or BSIG”) establishes the Federal Office for Information Security (BSI) and defines its tasks and competencies. The core task is to “prevent threats to the security of federal information technology” (see Section 3, Paragraph 1, Number 1, BSIG).

In 2015, Germany passed the IT-Security Law ("Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ or short „IT-Sicherheitsgesetz“). This law already implemented a vast majority of the requirements and rule sets that were later foreseen by the NIS-directive. The IT-Security Law is a so-called “Artikelgesetz”, i.e., a law that establishes, amends or changes several exiting German laws. In particular, it introduces modifications to the before mentioned BSI-Act has been adapted. Further changes address inter alia laws in the fields of telecommunication, energy, and social security.

In 2017, the “ Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“ implemented the NIS-directive in German law, again by amending and changing exiting German legislation, in particular the before mentioned BSI-Gesetz. Other adaptations address inter alia laws in the fields of telecommunication, energy and social security sector.

Germany has a law that regulates numerous aspects of the energy industry (in German “Energiewirtschaftsgesetz” or in short “EnWG”), in particular electricity and gas suppliers). Concerned enterprises are mandated to ensure the reliability and security (including IT-security) of their infrastructure such as energy networks (see Sections 49 et seq. EnWG).

The „Verordnung zur Bestimmung Kritischer Infrastrukturen“ (BSI-KritisV) lists categories of entities and companies considered to operate critical infrastructures for each sector that is addressed by European or German legislation. It has not been passed as an act of the parliament, but rather by the executive branch.

The "Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code", in its Article 40, contains norms on the security of networks and services. This directive has been implemented in Germany inter alia by revising the "Telekommunikationsgesetz" (TKG) and the "Telemediengesetz" (TMG).

The „Telekommunikationsgesetz" (TKG),in Sections 108 to 115, contains norms on the security and public security that apply to telecommunication providers.

The "Telekommunikationsmodernisierungsgesetz" will revise the TKG going into effect on 1st December, 2021. The aforementioned norms on security and public security in the TKG that apply to telecommunication providers will then be located in Sections 164 to 183 TKG-2021.

The „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien" (TTDSG) attempts to consolidate the regulations on data protection in the fields of telecommunication and telemedia within a single act. To this effect, it moves existing provisions that are currently spread over the TKG and TMG into the new TTDSG. At the same time, the provisions will apply changes made necessary by the GDPR and in once case, by the ePrivacy directive (2002/58/EC).

See Sections 11 et seq. TMG for data protection and Section 13 Paragraph 7 TMG in particular for the duty of the service provider to implement appropriate technical and organizational measures to protect personal data and to safeguard the availability of the service.

The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. The stipulation Article 32 GDPR is directly applicable to most entities and processing activities in Germany. It is also repeated accordingly in the federal data protection act (section 64 BDSG). Similar stipulations are part of the data protection acts of the federal states.

The German Federal Office for Information Security (BSI) has the authority to examine the security of information technology (see Section 7a, BSIG) and to issue standards for the minimal security of information technology (for example, in the form of guidelines). Please note that the BSI has specific competencies for the public entities of the federal sector and certain private entities, such as those who operate critical infrastructures the energy or telecommunication sectors. While not directly applicable to other private companies or persons, these guidelines have the potential to raise IT-security also in these excluded sectors.

11.3.2 Implementation of EU Law

(i) Are any particular procedures described in your national regulation?

German legislation is traditionally kept technology-neutral and thus it is unlikely for laws and statutes to refer to any particular procedures or measures except as examples. For instance, in the field of data protection, pseudonymization is stated as a typical example of a measure without excluding other or alternative measures that may be more effective.

The German BSI published a series of catalogues of measures which constitute a part of the BSI's "management system for information security" (ISMS) that is called "IT-Grundschutz" in German. IT-Grundschutz covers technical, organisational, infrastructural,

and other specific aspects. It offers a systematic approach to information security that is considered compatible to ISO/IEC 27001. Some core documents are also available in English language.[114] The broad set of catalogues with specific measures ("Bausteine") is available in German language.[115]

(ii) What is the status of the implementation of the NIS directive in your country towards data protection/security of data?

The German legislator had anticipated the NIS directive and passed the IT-Security Act ("IT-Sicherheitsgesetz") already in 2015 on the basis of the ongoing European discussion on the NIS directive. Where the final NIS directive deviated from the German law and thus required modifications, these were consequently implemented in 2016 by the Implementation Act for the NIS directive ("Umsetzungsgestz zur NIS-Richtlinie").

(iii) The GDPR stipulates that appropriate technical and organisational measures to protect personal data must be implemented. Is this prevention reflected in your national regulation?

The requirement to have appropriate technical and organizational measures in place are part of the German data protection legislations at both, federal and state level, as well as part of several sector-specific laws. Please refer to the tables in this section for examples and references.

11.3.3 Personal Data Breach Notification

(i) What requirements in relation to data breach notifications exist in your national regulation? Is this issue regulated in the national implementation of the NIS Directive?

Besides Articles 33 and 34 GDPR which are directly applicable, corresponding requirements which substantiate the GDPR for specific sectors of application can be found in Sections 65 and 66 BDSG, as well as in the Data Protection Acts of the federal states.

Personal data breaches have to be reported to the data protection authority competent for the controller. Sector-specific legislation at federal and state level may require additional institutions to be informed. For example, data security breaches that occur at social service authorities must not only be notified to the competent data protection authority, but also to the according legal supervision body (see e.g. Section 83a SGB X).

For IT-security breaches, the BSI is the central office for incident reports filed by all federal offices (see Section 4 BSIG). The BSI is also the central office for incident reports by critical infrastructure providers (see Section 8a Paragraph 4 BSIG). Providers of public telecommunication services have to report incidents to both, the BSI and the Federal Network Agency ("Bundesnetzagentur", see Section 109 Paragraph 6 TKG).

11.3.4 Supervision of cybersecurity

(i) Does a supervisory body in a narrow sense with enforcement powers exist in your country?

[114] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html.

[115] See https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html.

The BSI has the necessary enforcement powers for IT-security breaches. Sector-specific supervisory bodies such as the federal network agency also have enforcement powers in their field of jurisdiction.

(ii) Is in your country an institution like the German BSI (Bundesamt für Sicherheit in der Informationstechnik) established. The Federal Office for Information Security is the national cyber security authority of Germany. It shapes information security in digitisation through prevention, detection and reaction for government, business and society. (https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html) or something similar established? If yes, what are the competences and responsibilities?

The BSI is the German institution mentioned in the question. See also the answers to the questions above regarding the competencies of the BSI.

The Directive 2016/680 of 27 April 2016 "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" has been enacted into German national law. To this effect, an omnibus act was passed that re-structures the German Federal Data Protection Act (BDSG) and a series of other federal laws.

(iii) How can damages caused by a lack of cybersecurity be claimed (and compensated)? Are such issues sufficiently regulated in your country?

In case of personal data breaches, Article 83 GDPR and its according implementations in the BDSG as well as state-level data protection acts apply.

Compensation for a damages incurred due to a lack of cybersecurity are covered by general principles of law. Civil law provides for contractual damages (see Section 280 BGB) as well as for torts (see Section 823 BGB). In general, some fault is necessary on part of the debtor. This can be any breach of duty for contractual claims or, where the claims are based on tort, either wilful misconduct or negligence.

It may be noteworthy that in the case of gross negligence on part of an insured company or entity, the insurer may have the right to reject or reduce insurance payments (see Section 81 Paragraph 2 Versicherungsvertragsgesetz). This may for example be the case where evidentially necessary precautions failed to be implemented. So besides legal requirements to have IT-security measures in place the risk to loose insurance coverage in case of an security incident can be an incentive to take sufficient measures.

11.4 Enforcement: fines and sanctions

(i) Is a crime related to data protection or cybersecurity punished by a fine or imprisonment?

Regarding applicable law in Germany, sanctions and procedure against offences are regulated centrally in the OWiG ("Ordnungswidrigkeitengesetz" for administrative offences and misdemeanours) and StGB ("Strafgesetzbuch") and the Criminal Procedure Code (Strafprozessordnung) for criminal offences. Punishable offences concerning handling of data and cybersecurity are part of these acts as well as spread over several laws concerning specific matters. Examples for the latter include Social Security Acts (Sozialgesetzbuch, in particular SGV X and SGB V).

Regarding data protection, Sections 41 through 43 BDSG contain further details on sanctions for both, administrative and criminal offences related to data protection. Offences regulated in Article 83 (3) through (6) GDPR are treated as administrative offences.

Several statutory (criminal) offences in the German Criminal Code (Strafgesetzbuch, StGB) are related to data protection and Cybersecurity in a wider sense. In particular, Sections 200 201a, and 202 address violations of the privacy of spoken word, of correspondence and violation of the intimate privacy by taking images. Sections 202a, 202b, 202c and 303a StGB relate to unauthorized access and manipulation of data while Section 203 StGB foresees punishment for a breach of professional secrecy.

Also state-level data protection laws contain prescriptions about both, administrative and criminal sanctions. Laws from different federal states may deviate from each other. One difference is for example whether public entities can be fined; some states render this possible, while others completely exclude it, and yet others foresee it only for public entities who engage in commercial activities. The maximal fines for administrative offences are typically 25'000 € for formal offences and 50'000 € for material offences, respectively. The maximum imprisonment is two years. In some federal states, also the attempt of an offence is punishable. Certain federal states also regulate administrative offences that lack an equivalent in the GDPR or the German federal law (i.e., BDSG); for example, Niedersachsen sanctions employees or processors who abuse data processed by public entities.

An addition to state-level data protection laws, there is also a wide range of sector-specific laws that regulate offences related the processing of data that violates one of their obligations or prohibitions.

Missing or insufficient technical and organisational measures by critical infrastructure operators and other violations of obligations related to cybersecurity may be fined up to 2 million Euros, see Section 14 BSIG.

(ii) Are there administrative fines related to data protection issues?

Yes, both the federal and the different state-level laws foresee administrative fines (see also (i) above).

(iii) Do data protection offences constitute an official offence or are only prosecuted by the injured party's request?

Prosecutors can either act on request by injured parties or by a data protection authority. In particular, criminal offences listed in the Federal Data Protection Act (BDSG) are only prosecuted on request by an injured party or the Federal Data Protection Commissioner; offences listed in a Data Protection Low of the federal states are prosecuted on request by the injured party or by the Data Protection Commissioner of the respective federal state (except for the State of Sachsen).

11.5 Governance

(i) At least in the biomedical sciences, research involving human participants usually is subject to ethical review by research ethics committees or similar bodies. Data protection, however, not only affects the biomedical sciences, but potentially all fields of research. Are you aware of any committees (e.g. research ethics committees, ethical review boards) or agencies (e.g. national research funding agencies, national security agencies) in your country that review data protection issues in research projects? If yes, are reviews mandatory and governed by specific

guidelines or regulations? Do you know which aspects of data protection review bodies focus on? Are reviews only conducted before the actual research starts or is the research process monitored as well?

In Germany, a variety of ethics committees have been established in various fields of application and at both, the federal and state level.

The German Ethic Council (Deutscher Ethikrat) was founded based on the Federal Ethics Council Act (Ethikratgesetz). As an independent council of experts, it supports the German Bundestag and the federal government through opinions. The council can act both, on request by the Bundestag and on its own initiative. It may also inform the public and promote public discussion. The Council is active in the areas of ethical, social, scientific, medical, and legal issues. It can also occupy itself with the likely consequences of research and development activities for individuals or society as a whole. This is especially relevant in the field of life sciences and their application to humans (see Section 2 Ethikratgesetz).

Also the federal states passed legislation to establish ethic commissions. These have been funded inter alia at universities (based on the federal states' University and College Acts, "Hochschulgesetze") and at various professional chambers (at least the chambers of medical professions, based on the "Heilberufekammergesetze" or "Kammergesetze" of the States).[116] Where federal and state law mandates consultations outside of university research, usually the commissions of these professional chambers get involved. For example, clinical trials in the area of drugs and medical appliances require prior consultation of an ethics committee (see Section 42 of the German Medicines Act, "Arzneimittelgesetz" and Section 32 et seq. of the Implementing Act for Regulation 2017/745 on Medicinal Devices, "Medizinprodukterecht-Durchführungsgesetz").

To my knowledge, in Germany, data protection and informed consent are often object of the assessments by ethics committees. This is conducted predominantly from the perspective of ethics, however; it may thus differ from an assessment that focusses on data protection legislation. The assessment of compliance with data protection legislation mostly remains in the hands of the data protection officers of the institutions who conduct research.

(ii) What instruments (e.g. ethics self-assessments at the proposal stage), if any, do research funding agencies and other research supporting bodies in your country use to promote data protection in ICT R&I? Do they facilitate the use of these instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

For research proposals, German funding institutions may require an ethics assessment and/or an evaluation by an ethics board. For example, the "Deutsche Forschungsgemeinschaft" (DFG) asks to accompany proposals with a self-assessment to identify any potential risks/harm to individuals together with a specification on how these are mitigated. In some kinds of proposals, such as those involving experiments on humans or dual-use research, an ethics statement is always required. The proposal preparation instructions by DFG provide some guidance in this respect.[117] Depending on the area of research, other funding institutions have similar requirements.

[116] For a non-exhaustive list of medical ethics committees see e.g., the list of members the working group of medical ethic commissions (Arbeitskreis Medizinischer Ethik-Kommissionen), https://www.akek.de/en/ethik-kommissionen/.

[117] See: https://www.dfg.de/formulare/54_01/index.jsp.

The author has found no indication that German research funding agencies (or other research supporting bodies) facilitate data protection by means of particular tools, or guidelines for the implementation-phase of research projects. That said, German funding institutions at federal and state level increasingly incorporate ethical, legal, and social aspects (ELSA) into their funding programs. This can either constitute projects of their own focussing on data protection research, parts of projects (e.g., as a work package), or calls for coordination and support activities that run alongside a set of research initiatives with a common topic (e.g. the project "Assessing Big Data" ABIDA[118] as an interdisciplinary research project on legal, ethical and economical aspects of big data). A long-lived and cross-sectional and interdisciplinary project which addresses data protection from various angles is the project "Privacy Forum and Self-determined Life in the Digital World"[119] which is funded by the Federal Ministry for Education and Research.

(iii) Are there any national regulations or procedures that specify what to consider when ICT R&I involves defence technology, dual use technology or is affected by embargoes? If yes, who are the bodies responsible for monitoring and enforcement? Are there any tools researchers and innovators working on security-sensitive technologies can use in order to protect against industrial espionage and other confidentiality breaches?

The author is not aware of specific national procedures and regulations applicable to ICT R&I but the University and College legislation of several federal states and the public research institutions themselves have limitations on research with dual use potential. In Germany, the EU Dual Use Regulation (EC) 428/2009 is applicable, however. The body responsible for its enforcement is Federal Office for Economic Affairs and Export Control ("Bundesamt für Wirtschaft und Ausfuhrkontrolle", BAFA). The BAFA published guidelines titled "Export Control in Science & Research" as well as the "Export Control and Academia Manual".[120]

Regarding the protection against industrial espionage, the author is unaware of any particular tools. Guidance and support for researchers in academia and industry is available from the Offices for the Protection of the Constitution ("Verfassungsschutzamt") at both, federal and state level. All institutions and offices in charge of counter intelligence also offer advice, guidelines, and instructions to researchers and businesses.

12 Greece

Irene Kamara (Tilburg University)

12.1 Informed consent

12.1.1 General Regulatory Framework

[118] See https://www.abida.de/en.
[119] See https://www.forum-privatheit.de/en/.
[120] Download page for both publications, https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Academia/academia_node.html.