

instruments or data protection impact assessments by providing tools (software or other), templates or guidelines?

Mostly through submitting documents at proposal stage. Submitting a data management plan (DMP) is often required.

For certain documents, online tools are recommended, i.e. the Data management tool DMP online for creating data management plans. The agencies provide DMP templates<sup>51</sup> or link to online tools for data management.

(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?

No specific national legislation for dual-use of ICT technology has been found.

## 2 Belgium

Gianclaudio Malgieri, Andrés Chomczyk (BUV)

### 2.1 Informed consent

#### 2.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law...)	Brief description and scope
<b>Loi du 3 décembre 2017 portant création de l'Autorité de protection des données</b>	<a href="https://bit.ly/2SleXOW">https://bit.ly/2SleXOW</a>	Hard law	This organic law regulates the structure and composition of the Belgian Data Protection Authority
<b>Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (the</b>	<a href="https://bit.ly/31vnYIH">https://bit.ly/31vnYIH</a>	Hard law	Implementation of GDPR in Belgium

<sup>51</sup> <https://www.fwf.ac.at/de/forschungsfoerderung/open-access-policy/forschungsdatenmanagement/>, accessed 3.6.2020

“Belgian Data Protection Act”)			
Regulation	Link (English version if possible)	Type of regulation (hard law, soft law...)	Brief description and scope
Loi du 3 décembre 2017 portant création de l’Autorité de protection des données	<a href="https://bit.ly/2SleXOw">https://bit.ly/2SleXOw</a>	Hard law	This organic law regulates the structure and composition of the Belgian Data Protection Authority

**Main regulatory tools addressing data protection issues and informed consent in Belgium**

- (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?

No, under the Belgian Data Protection Act there are no rules prescribing how data process for purely personal or household activity should be processed.

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

Yes, the Belgian Data Protection Act stipulates how data should be processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security in its Title 2.

Moreover, Title 3 prescribes how other government agencies and the military have to process personal data. In this sense, Subtitle 1 is applicable to intelligence and security services, Subtitle 2 to armed forces, Subtitle 3 for classification and security clearances, security certificates and security recommendations, Subtitle 4 to the Coordination Unit for Threat Assessment -terrorism fighting government agency- and Subtitle 5 to the Passenger Information Unit.

Name of Authority	Link (English version if possible)	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made by the public
De Gegevensbeschermingsautoriteit (NL) L’Autorité de protection	<a href="https://www.dataprotectionauthority.be/">https://www.dataprotectionauthority.be/</a>	Yes	Currently, the Belgian DPA has 17 members among its direction committee, its	In our opinion, the Belgian DPA has an active role	The Belgian DPA seems to be responding

<p><b>des données (FR)</b></p> <p><b>Die Datenschutzbehörde (DE) (the “Belgian DPA”)</b></p>			<p>knowledge centre and its litigation team. Besides this, in latest information annual report (2018 report) it was stated that there were 59 administrative members.</p>	<p>in the country.</p>	<p>to the claims filed by individuals as well as developing guides regarding data protection for individuals.</p>
--	--	--	---	------------------------	---

**Information regarding Data Protection Authority, Belgium.**

- (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.?

No, the Belgian Data Protection Act doesn’t introduce a specific definition of “data processing for research purposes”.

The Belgian legislation doesn’t define “research in public interest”. However, the Belgian DPA stated in its comments to the draft bill of the Belgian Data Protection Act that this provision of the GDPR can comprehend certain activities carried out by private entities and not only research done by public institutions<sup>52</sup>.

- (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?

Yes, Articles 190 through 192 and 198 through 204 of the Belgian Data Protection Act stipulates further measures that data controllers and data processors must adopted. In particular, it is developed how anonymization and pseudonymization should be adopted in regard to research purposes.

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

Yes, Article 9 of the Belgian Data Protection Act prescribes that when processing genetic, biometric or health-related data, data controllers should “designate the categories of persons who have access to the personal data, and shall meticulously describe their capacity with regard to the processing of the data concerned (...) keep the list of the as so designated categories of persons at the disposal of the competent supervisory authority (...) ensure that the designated persons are bound by a legal or legal obligation or by an equivalent contractual provision to respect the confidential nature of the data concerned”.

<sup>52</sup>[https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/avis\\_52\\_2018\\_0.pdf](https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/avis_52_2018_0.pdf)

Moreover, Article 206 of the Belgian Data Protection Act prescribes that special category of data (under article 9.1 of the GDPR) cannot be disseminated for research or statistical purposes, not even in a pseudonymized manner.

- (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.)?

As of the date hereof, no code of conduct related to data processing in research has been approved by the Belgian DPA.

In spite of this, several Belgian institutions have enacted a joint code of ethics for the scientific research activity<sup>53</sup>. However, this code of ethics doesn't deal with any data processing issue.

We were able to identify a guideline applicable to medics issued by the Ordre des médecins and titled "Récolte et exploitation de données médicales"<sup>54</sup>. This guideline is applicable to any data collection activity carried out by medics in Belgium, including when it was done for research purposes. It mandates that medics have to inform patients about the data processing activities. As for the legal basis, it encourages medics to collect consent but recognizes that other legal basis might be used for certain purposes, such as research. Regarding the purposes, the guideline indicates that data shouldn't be reused. Among the security measures recommended, the guidelines mandate the use of anonymization techniques. As for prohibitions, the guidelines forbid medics from benefiting from the commercialization of their patient's data.

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

The Belgian Data Protection Act doesn't provide a specific definition of data processing for statistical purposes. Nevertheless, the Belgian Data Protection Act does provide for specific rules that apply to such data processing which are the same as for "data processing for research purposes" in Title 4.

- (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.)

No, to the best of our knowledge and besides the aforementioned obligations, there are no other references to data processing for research purposes in the national legislation.

### 2.1.2 Rights of data subjects and data processing

- (i) 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.)

Yes, the Belgian Data Protection Act provides for certain data subjects, in accordance with Article 4.2, all those individuals who are on Belgian territory if the data was collected for the purposes of "the offering of goods or services to such data subjects on

---

<sup>53</sup> [http://www.belspo.be/belspo/organisation/publ/pub\\_ostc/Eth\\_code/ethcode\\_fr.pdf](http://www.belspo.be/belspo/organisation/publ/pub_ostc/Eth_code/ethcode_fr.pdf)

<sup>54</sup> <https://www.ordomedic.be/fr/avis/conseil/r%c3%a9colte-et-exploitation-de-donn%c3%a9es-m%c3%a9dicales>

Belgian territory, irrespective of whether a payment of the data subject is required; or the monitoring of their behaviour as far as their behaviour takes place on Belgian territory”.

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

No, there are no special requirements regarding informed consent at the national level. Nevertheless, the Belgian DPA has provided some informative material to the general public regarding the obligations concerning consent in the GDPR and the Belgian Data Protection Act<sup>55</sup>.

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

Yes, the Belgian Data Protection Act prescribes special requirements for certain data processing activities, mainly those carried out by government agencies involved in crime investigation and prosecution as well as those related to national security and the military. In fact, the bulk of the Belgian Data Protection Act revolves around the special conditions that should be address by those entities when processing personal data related to their purpose.

As an example, the principle of transparency, in accordance with Article 14 of the Belgian Data Protection Act, doesn't apply to “the processing of data originating, whether directly or indirectly, from the judicial authorities, the police services, the General Inspectorate of the Federal and Local Police, the Financial Intelligence Processing Unit, the General Administration of Customs and Excise Duties and the Passenger Information Unit”.

In this regard, the special conditions set forth by the Belgian Data Protection Act provide for less transparency in the eyes of the data subject but stricter obligations for the data controllers and data processors in these data processing activities. In particular, the safeguards that should be adopted to protect the personal data in their possession are prescribed by other regulations and not left at the criteria of the data controller or data processor, as applicable.

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

Yes, the Belgian Data Protection Act have certain particularities regarding data subjects' rights.

First, when the data subject rights are exercised before the entities indicated in Title 3<sup>56</sup> or before other data controllers that have shared, directly or indirectly, data with those entities, the request will be relayed to the Belgian DPA to be processed.

Secondly, in certain situations prescribed in the Belgian Data Protection Act, it shall be necessary the intervention of the Belgian DPA to determine if the data subject can exercise her rights.

Third, in accordance with Article 16 of the Belgian Data Protection Act “where the personal data are mentioned in a judgment or judicial file, or are processed in the context of criminal investigations and proceedings, the rights referred to in Articles 12 to 22 and

---

<sup>55</sup> <https://www.youtube.com/watch?v=9Ql4A0aWObg>

<sup>56</sup> Intelligence and security services, armed forces, entities that provide classification and security clearances, security certificates and security recommendations, the Coordination Unit for Threat Assessment and the Passenger Information Unit.

34 of the Regulation shall be exercised in accordance with the Judicial Code, the Code of Criminal Procedure, the special laws governing criminal procedure and their implementing decrees”.

### 2.1.3 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)?

Yes, the Belgian Data Protection Act has special provisions for processing special categories of personal data.

In this regard, Article 8 of the Belgian Data Protection Act states that the following purposes shall be considered as substantial public interest: (i) defend and promote human rights and fundamental freedoms by entities incorporated for that purpose and authorised by the King, by decree deliberated in the Council of Ministers, after advice of the competent supervisory authority; (ii) activities carried out by the ‘Fondation pour Enfants Disparus et Sexuellement Exploités’; and (iii) activities carried out by associations with legal personality or foundations whose principal legal objective is to assess, supervise and treat persons whose sexual behaviour can be qualified as an offence and which, for the purpose of achieving that objective, are approved and subsidized by the competent authority. In connection with the last purpose, those entities cannot process genetic or biometric data for identification purposes.

Moreover, and as stated above, Article 9 of the Belgian Data Protection Act implements Article 9.4 of the GDPR.

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

Yes, the Belgian Data Protection Act has special rules when processing personal of children. In this regards, Article 7 states that “(...) the processing of personal data related to children in relation to the offer of information society services directly to a child is lawful where the consent has been given by children who are at least 13 years old. Where the processing concerns personal data of a child below the age of 13 years, such processing shall be lawful only if that consent is given by the child’s legal representative.”

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

No, there are no other vulnerable individuals identified in the Belgian Data Protection Act.

### 2.1.4 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?

The Belgian Data Protection Act doesn’t contemplate regulation for the personal data of a deceased individual.

### 2.1.5 Accountability and Data Protection Impact Assessment

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

No, the Belgian Data Protection Act doesn't introduce further provisions related to accountability.

- (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?

Yes, in the Belgian Data Protection Act there are specific requirements regarding data protection impact assessments.

First, Article 23 of the Belgian Data Protection Act stipulates that, even if a prior data protection impact assessment was done when passing the legislation that serves as legal basis, a data protection impact assessment must be carried out when the processing is based on Articles 6.1.c or 6.1.e and it must be considered at high risk under Article 35 GDPR.

Second, in connection with data processing activities carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, Article 58 of the Belgian Data Protection Act prescribes the minimum issues that should be contemplated by those data controllers when carrying out a data protection impact assessment. Article 65.3 of the Belgian Data Protection Act indicates that the data protection officer shall provide advice when requested in connection with the aforementioned data protection impact assessment.

Third, in the case of data processing activities conducted by intelligence and security services, Article 92 of the Belgian Data Protection Act states that a data protection impact assessment shall not be a prerequisite for the communication of personal data between an intelligence and security service and any public or private body. The same exemption is applicable to the same kind of transfer done in the context of processing of personal data in the context of the Act of 11 December 1998 on classification and security clearances, security certificates and security recommendations, in accordance with Article 125 of the Belgian Data Protection Act, as well as to transfers done in the context of processing of personal data by the Coordination Unit for Threat Assessment, in accordance with Article 158 of the Belgian Data Protection Act.

In the case of data processing in research, Article 191 of the Belgian Data Protection Act indicates that a data protection impact assessment, if necessary, according to the requirements set forth by the GDPR, shall be considered as a general safeguard as required by Article 89 of the GDPR

## 2.2 Commercialization of data

### 2.2.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law...)	Brief description of and scope
------------	------------------------------------	--	--------------------------------

<p><b>Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (the “EU Regulation on Free Flow of Non-Personal Data”)</b></p>	<p><a href="https://bit.ly/38fYhi2">https://bit.ly/38fYhi2</a></p>	<p>Hard law</p>	<p>European regulation not implemented in the Belgian legal framework yet</p>
<p><b>Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (the “EU Directive on Contracts of Digital Content and Services”)</b></p>	<p><a href="https://bit.ly/37e9Vsj">https://bit.ly/37e9Vsj</a></p>	<p>Hard law</p>	<p>European directive not implemented in the Belgian legal framework yet</p>
<p><b>Belgian Data Protection Act</b></p>	<p><a href="https://bit.ly/31vnYIH">https://bit.ly/31vnYIH</a></p>	<p>Hard law</p>	<p>Implementation of GDPR in Belgium</p>
<p><b>Loi portant insertion du Livre XI "Propriété intellectuelle" dans le Code de droit économique, et portant insertion des dispositions propres au Livre XI dans les Livres I, XV et XVII du</b></p>	<p><a href="https://bit.ly/3bsK4jV">https://bit.ly/3bsK4jV</a></p>	<p>Hard law</p>	<p>Belgian legislation creating copyright rights over databases</p>

<b>même Code (the “Belgian Database Copyright Act”)</b>			
<b>Loi relative à la protection des consommateurs en matière de contrats d'utilisation de biens à temps partagé, de produits de vacances à long terme, de revente et d'échange (the “Belgian Consumer Protection Act”)</b>	<a href="https://bit.ly/37hRAuu">https://bit.ly/37hRAuu</a>	Hard law	Belgian legislation regarding consumer protection in general

**Main regulatory tools addressing data commercialization in Belgium.**

**2.2.2 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)?

Since there are no special regulations about contract for the supply of digital services or digital contents (apart from the direct application of EU Directive on Contracts of Digital Content and Services, not implemented in Belgium yet), there are no specific rules about that, not even in Belgian Consumer Protection Act.

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

To our best knowledge, this practice is performed, in accordance with the EU Directive on Contracts of Digital Content and Services.

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

No, it does not. The only applicable rules concern personal data protection and follow the GDPR principles, without any further specification about remuneration of data subjects.

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

No, there is not.

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

The EU Regulation on Free Flow of Non-Personal Data about the processing of non-personal data still needs to be implemented in the Belgian legal system.

### 2.2.3 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?

To the best of our knowledge, there is no specific definition of data as commodity or good in any national piece of legislation.

- (ii) 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?

Copyright (droit d’auteur) is regulated by Section 4 (Articles 46-47) of the Belgian Database Copyright Act. However, to the best of our knowledge, there is no specific mechanism to determine the value of data

## 2.3 Security and cybersecurity

### 2.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law...)	Brief description and scope
<b>Loi établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique (the “Belgian NIS Act”)</b>	<a href="https://bit.ly/2vb5vF1">https://bit.ly/2vb5vF1</a> (FR)	Hard law	Transposition of NIS Directive
<b>Arrêté royal portant création du Centre pour la Cybersécurité Belgique (the “Belgian CPC Act”)</b>	<a href="https://bit.ly/2S7INao">https://bit.ly/2S7INao</a>	Hard law	Creation of the Centre for Cybersecurity Belgium

### Main regulatory tools addressing security and cybersecurity in Belgium

#### 2.3.2 Implementation of EU Law

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

The Belgian Data Protection Act doesn’t provide for any particular procedure regarding the implementation of security measures. Accordingly, the determination of such security measures should be adopted to the data controllers and data processors.

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

The NIS directive has been transposed into Belgian regulation as the Belgian NIS Act on April 7, 2019 and published on the Belgian Official Gazette on May 3, 2019.

- (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?

Yes, the Belgian Data Protection Act imposes certain technical and organisational measures when data is being processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose as discussed previously in this report.

Besides this, the Belgian NIS Act mandates, in Article 21, that operators of essential services need to deploy security measures that meet, at least, the level set forth by ISO / IEC 27001 or a national, foreign or international standard recognized as equivalent by the King, by decree deliberated in the Council of Ministers. Moreover, Article 33 prescribes that digital service providers shall adopt the necessary measures to identify and mitigate risks that threaten the security of the network and information systems used for the delivery of their services.

### 2.3.3 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?

The Belgian Data Protection Act does have certain special regulations for data breach notifications in certain situations, mainly when the processing is covered by Title 2 and certain Subtitles of Title 3 that deal with data processing by government agencies related to crime and national security. While the Belgian Data Protection Act doesn't expand the requirements set forth by the GPDR in regard to the content of the communication dealing with the data breach, it does prescribe to whom the notification has to be deliver. In particular, intelligence and secret service agencies acting as data controllers do not need to notify the data breaches to the Belgian Data Protection Agency, but to "Standing Committee I", i.e. the Standing Intelligence Agencies Review Committee.

As for the Belgian NIS Act, there are special regulations for both essential service providers, Articles 35 through 37, and digital service providers, Articles 24 through 31. While the content of the notification doesn't differ much from the content required for a data breach notification, it does change, in comparison to the GDPR and the Belgian Data Protection Act, the receipt of the notification. In the case of essential service providers, the notification has to be done to (i) the national CSIRT, (ii) the sectorial authority/sectorial CSIRT and (iii) to the Centre for Cybersecurity Belgium; if the entity provides infrastructure for the financial system, then it also has to include the National Bank of Belgium, among the recipients of the notification. As for the providers of digital services, they only need to communicate to the first three entities mentioned.

### 2.3.4 Supervision of cybersecurity

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

In regard to the Belgian Data Protection Act, the Belgian DPA can enforce the provisions of both the GDPR and the Belgian Data Protection Act and impose administrative penalties. Moreover, the Belgian Data Protection Act provides for criminal penalties that can be prosecuted by the Public Prosecutor Office.

On the other hand, the Belgian NIS Act states that the inspection services of the relevant sector or sub-sector, if applicable, can open case files due to violations of the aforementioned regulation. If the case file results in the existence of a violation to the Belgian NIS Act, then the case file can be transferred to the Public Prosecutor Office for the application of administrative sanctions. Moreover, the Belgian NIS Act criminalizes violations of certain obligations in the Belgian NIS Act. In these cases, general criminal law rules apply.

- (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](https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html)) or something similar established? If yes, what are the competences and responsibilities?

Yes, the Centre for Cyber Security Belgium is the institution in charge of shaping information security in Belgium.

Its competences and responsibilities are detailed in Belgian CPC Act

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

The Belgian NIS Act doesn't contemplate the possibility of claiming damages for harms caused by lack of cybersecurity measures.

Nevertheless, Article 82 of the GDPR is applicable in case damages are claimed. As of the date hereof, there are no active casefiles on the matter.

## 2.4 Enforcement: fines and sanctions

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

Yes, both the Belgian Data Protection Act and the Belgian NIS Act stipulate criminal sanctions for certain actions related to the relevant statutes.

In the case of the Belgian Data Protection Act, the criminal provisions range from malicious or negligent non-compliance with the regulation through disregarding orders from the Belgian DPA up to forging documents to obtain authorizations or certifications related to certain data processing activities such as code of conducts. It is important to indicate that none of the criminal provisions carry an imprisonment punishment as all of the sanctions are monetary fines.

As for the Belgian NIS Act, the criminal sanctions provided in that statute also revolve around the non-compliance of the regulation. However, in the case of the Belgian NIS Act, there are imprisonment punishments for the commission of the crimes prescribed therein.

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

Yes, both the Belgian Data Protection Act and the Belgian NIS Act stipulate administrative fines for the non-compliance with the corresponding regulation.

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

The criminal offences prescribed in the Belgian Data Protection Act and the Belgian NIS Act are considered as official offences and, therefore, can be freely initiated by the public prosecutor. Both regulations have special regulations in place for when a criminal offence might also qualify as an administrative offence in order to coordinate all actions between the administrative authority and the public prosecutor.

### 2.5 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 Belgium there is the Belgian Advisory Committee on Bioethics<sup>57</sup>, established by the co-operation agreement of 15 January 1993 (FR-NL version) signed by the federal Government, the French-speaking Community, the Flemish Community, the German-speaking Community and the Joint Commission for Community Matters. The Committee is completely independent of the authorities that created it.

The Committee has a twofold mission: a) to provide opinions on the problems raised by research and research applications in the fields of biology, medicine and health care. The ethical, social and legal aspects of these problems are studied, particularly from the angle of respect for human rights; b) to inform the public and the government authorities about these problems.

In order to fulfil this mission, the Committee is legally obliged to: make an annual report of its activities (Fr version), organize a biennial public conference (events), manage a documentation centre.

Actually, such committee is specialized in the following topics: health, food, animals and environment. Accordingly, there is no specific unit dedicated to personal data protection.

- (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?

Generally, all data controllers (in particular if public entities) carrying out research have:

- A data protection officer according to the GDPR and
- A Research Ethics Committee (usually at University level or at professional orders level). In particular, a special Ethics Committee is required, e.g., at Article 11 of the

---

<sup>57</sup> <https://www.health.belgium.be/en/belgian-advisory-committee-bioethics>

Law 7 May 2004 on experiments on human persons (Loi relative aux expérimentations sur la personne humaine).

Both the DPO and the Research Ethics Committees deal with legal and ethical compliance about data protection in research.

As regards the DPIA, the Belgian DPA has developed a blacklist and whitelist for data processing in need of DPIA.<sup>58</sup> However, to our best knowledge, there is no other specific tool for researchers to carry out DPIA or other data protection safeguards.

- (iii) As regards the DPIA, the Belgian DPA has developed a blacklist and whitelist for data processing in need of DPIA.<sup>59</sup> However, to our best knowledge, there 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?

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?

As regards dual use, the General EU Council Regulation (EC) N. 428/2009 of 5th May 2009 about dual use is implemented by Articles 6 and 7 of the Flemish Government Decree of 14 March 2014 regulating export, transit and transfer of dual-use and the delivery of technical assistance (Belgian Official Gazette of 2 May 2014) and Articles 5 and 6 of the Walloon Government Decree of 6 February 2014 regulating export, transit and transfer of dual-use items and technology (Belgian Official Gazette of 19.2.2014)). These provisions require a special authorization for transit of listed dual-use items for military end use destinations.

As regards industrial espionage, researchers and innovators in Belgium can use the Belgian Act of 30 July 2018 on the Protection of Trade Secrets ('Act on Trade Secrets'). In addition, in most serious cases also Article 309 of the Penal Code (Code Pénal) can apply.

### 3 Bulgaria

Yordanka Ivanova (Sofia Bar Association/Sofia University)

---

<sup>58</sup> Autorité de protection des données, Liste des types d'opérations de traitement pour lesquelles une AIPD est requise, [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste\\_des\\_traitements\\_AIPD.pdf](https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf)

<sup>59</sup> Autorité de protection des données, Liste des types d'opérations de traitement pour lesquelles une AIPD est requise, [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste\\_des\\_traitements\\_AIPD.pdf](https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf)