organization, political party, organisation, movement or coalition with political objective, or because of his or of his next-of-kin political convictions

3. Offences prosecuted officially by the Prosecution (ex officio - no need for request/complaint by the injured party). All offences that are not explicitly prosecuted under point 1 or 2 are officially prosecuted. In principle, these include all serious offences such as computer crimes, document related crimes, fraud etc.

3.5 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?

As already mentioned in part 1 of the questionnaire, ethical codes and review boards normally exist within each university/research organisation, but these codes and board reviews usually don't focus on privacy/data protection issues except in the case of medical 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?

As already mentioned in part 1 of the questionnaire, state-funded research in Bulgaria needs to be ethical in principle, but in practice there are no special requirements or self-assessment tools that research projects have to undergo to comply with this general principle.

(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?

Not found in the existing public documents/legislation.

4 Croatia

Sunčana Roksandić Vidlička (University of Zagreb)

4.1 Informed consent

4.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope
Zakon o provedbi Opće uredbe o zaštiti podataka (Implementation Act of the EU General Data Protection Regulation) (25 May 2018)	https://translate.google.com/translate?hl=en&sl=hr&u=https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html&prev=search	Hard law	Aligns Croatian data protection law with the GDPR, but also offers provisions that differ from GDPR's requirements
Ustav Republike Hrvatske (Constitution of the Republic of Croatia)	https://azop.hr/images/dokumenti/266/theconstitutionoftherepublicofcroatia.pdf	Hard law	Guarantees safety and secrecy of personal data and notes data may be used without consent only under conditions specified by law
Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske (Act on Security-Intelligence System of the Republic of Croatia - ASIS)	https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Security%20and%20Intelligence%20System%20Act.pdf	Hard law	This act allows oversight over the work of security and intelligence agencies in protection of constitutional and legal rights of citizens
Zakon o kaznenom postupku (Criminal Procedure Act - CPA)	http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Procedure-Act.pdf	Hard law	Contains conditions and safeguards under which traffic and content data can be obtained and used

Zakon o zaštiti potrošača (Consumer Protection Act)	http://pak.hr/cke/propisi,%20zakoni/en/ConsumerProtectionAct/Consumer.pdf	Hard law	Croatian Consumer Protection Act contains a provision stating that 'the retailer shall be prohibited from providing personal data to any third party without the prior consent of the consumer, in accordance with the law governing the protection of personal data

Main regulatory tools addressing data protection issues and informed consent in Croatia

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

No, there are no provisions under Croatian law that apply purely to personal or household activity.

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

The security and intelligence system of the Republic of Croatia consists of two security and intelligence agencies: the Security and Intelligence Agency, and the Military Security and Intelligence Agency, whose activities are bound by the Croatian Constitution, ASIS, NSReg, the National Security Strategy, the Defence Strategy and the Annual Guidelines for the Work of Security Services. Their work is subject to scrutiny by the Croatian Parliament, the President of the Republic, the prime minister, ministers of defence and interior, the Office of the National Security Council and the Council for the civilian scrutiny of the security intelligence agencies. Act on Security-Intelligence System of the Republic of Croatia (ASIS) regulates protection of classified data and establishes the Information Systems Security Bureau (hereinafter: ZSIS) as the central state authority for the performance of functions in technical areas within the field of information security in state authorities of the Republic of Croatia.

Police Duties and Power Act (PDPA) states the Police are not empowered to conduct the interception of content data in the exercise of their duties and competences. They can only do so in the course of criminal proceedings, upon request and in accordance with the instructions given by the State Attorney and the courts.

The Electronic Communications Act (ECA) imposes an obligation on providers of communications services to keep subscriber information. Pursuant to Art. 108(5) ECA, service providers “must keep a list of end-users of their services, which they are obliged to deliver to the competent authorities …upon their request”. Such list must contain “all the necessary data enabling unambiguous and immediate identification of every end-user”.

Croatian GDPR Implementation act does not cover that topic.

Name of Authority	Link (English version if possible be)	Is this an independent body?	Number of employees	Level of activity (according to your appreciation)?	Response to requirements, questions, etc. made by the public
Agencija za zaštitu osobnih podataka (Croatian Personal Data Protection Agency)	https://azop.hr/data-protection-agency	Yes	In the latest report (25.5.2018), the number of registered data protection employees was 7.957	The Agency has an active role	The Agency responds to questions and claims made by the public, has a very useful webpage where the public can get informed about its work and publishes annual reports.

Information regarding Data Protection Authorities, Croatia.

(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 Croatian GDPR Implementation Act (Article 33) permits further processing of personal data for official statistical purposes under special rules governing official statistics if the data controller implements appropriate safeguards. Such data must not enable the identification of the person concerned. Croatian legislation does not define research in public interest, as it is defined in the GDPR, and the Implementation Act follows its provisions, but Croatian Personal Dana Protection Agency requested an explanation from the Croatian Bureau of Statistics for the purpose of obtaining personal information in regard to the Structure of payments research, and the Bureau explained that research that was defined by the Annual statistic activity plan of Republic of Croatia, and as such, does not differ from the requirements set in the GDPR.

(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, as previously mentioned, Article 33 of Croatian GDPR Implementation Act notes that the subjects whose data have been collected and processed for official state statistics activities are not given the right to access, right to rectification, right to limitation of

processing or right to objection in cases when the exercising of those rights would threaten or disable the state body in performing the statistic activities.[60]

(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, the Croatian GDPR Implementation Act introduces some further limitations beyond article 9 of the GDPR, regarding the genetic and biometric data processing. In Article 20 it prohibits processing genetic data to assess data subjects' illnesses or other health aspects relating to concluding or performing a life insurance agreement or an agreement with endowment clauses. In the same Article it expressly prohibits the use of consent as a legal basis to process genetic data for these purposes. Those prohibitions only apply when both the data subject executing the life insurance agreement or agreement with an endowment clause is in Croatia and/or the data controller is established in Croatia or provides services in Croatia. Regarding the processing of biometric data by public- and private-sector entities, including in the employment context, Article 22 states that private-sector entities may only process biometric data when either the applicable law requires the processing, data subjects' interests do not override the processing, which is necessary to protect individuals, property, classified information, or business secrets or for the individual and secure identification of service users. Private-sector data controllers must rely on service users' (data subjects') explicit consent as the legal basis for processing biometric data for the purpose of securely identifying service users. Public-sector entities may only process biometric data when both the applicable law needs the processing and data subjects' interests do not override the processing and the processing is necessary to protect individuals, property, classified information, or business secrets (Article 21). Public-sector data controllers do not need explicit data subject consent when the processing of biometric data is necessary to fulfil obligations arising under international treaties that relate to identifying individuals at state border crossings. The Croatian GDPR Implementation Act also permits public- and private-sector employers to process biometric data under certain circumstances (Article 23). Article 24 of the Croatian Act defines when the provisions on processing biometric data apply. [61] Any processing of information classified as a secret under a special law must be conducted in accordance with that law (Article 39(1), Croatian GDPR Implementation Act, which implements GDPR Article 90). Only officials holding a valid certificate required to access classified information can access, copy, or otherwise process information classified as secret under special laws.

(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.)?

The Croatian Committee on Ethics in Science and Higher Education (CESHE) was founded in 2005, by the Law on Science and Higher Education adopted by the Croatian Parliament. By the Law, CESHE is responsible for judging the alleged cases of research misconduct occurring in the public research and higher education system in Croatia and being submitted to the Committee, and promoting of ethical principles in science and higher education. The alleged research misconduct cases are judged with respect to the CESHE Code of Research Ethics and the respective codes of public universities and

[60] https://iapp.org/news/a/croatian-gdpr-implementation-law-main-features-and-unanswered-questions/
[61] https://www.babic-partners.hr/wp-content/uploads/2019/02/Croatian-implementation-of-GDPR.pdf

research institutes, which by law should be compliant to the CESHE Code. In addition, CESHE has an authority to provide public statements on research integrity misconduct and breaking of the Code by public research institutions (universities, faculties and research institutes) The investigations are carried out after the alleged cases are submitted by individuals or organizations or their ethical committees to CESHE. Then, the CESHE Chair verifies the alleged case in respect to the CESHE Code of Research Ethics and CESHE Rules of Procedure and presents the case to the CESHE members. Each alleged case is then taken by one CESHE member, who serves as a rapporteur to the CESHE. The rapporteur report is then discussed on regular CESHE sessions and the statement about the case is reached by majority of votes of CESHE members. If the expertise of CESHE members is not satisfactorily to judge the case, external expert members may be appointed. CESHE is not the decision-making body and is providing opinions on the processed cases on research misconduct. The decision on measures and sanctions coming out of CESHE statements is done by legal institutions on which the researcher/professor/other is employed.[62]

(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 Croatian GDPR Implementation Act does not provide a specific definition of data processing for statistical purposes. However, as aforementioned, in its Article 33 it does provide for specific rules that apply to such data processing.

(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.)

There is no special duty to have a DPO or DPIA in Croatia, except in the cases it is so instructed in the GDPR. However, the duty to collect consent whenever possible and necessary is strictly applied.

4.1.2 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, as aforementioned, data controllers are permitted to restrict certain data subject rights when they process personal data for official statistical purposes under applicable laws.

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

According to Croatian GDPR Implementation Act, consent is required for children under 16 years old (Article 19).

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

Under the Article 33 of the Croatian GDPR Implementation Act, certain GDPR Articles relating to data subjects' rights and data controllers' related obligations do not apply to processing for official statistical purposes, including the: Access right (Article 15, GDPR); Rectification right (Article 16, GDPR); Processing restriction right (Article 18,

[62] http://www.enrio.eu/news-activities/members/croatia/

GDPR); Objection right (Article 21, GDPR). These restrictions of data subjects' rights should be limited to situations where restricting data subjects' rights is strictly necessary to achieve the official statistical purpose and permitting data subjects to exercise their rights may hinder or impede achievement of the purpose.[63]

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

Yes, as mentioned in the previous answer.

4.1.3 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 Croatian GDPR Implementation Act includes additional requirements applicable to video surveillance of residential buildings and public areas in Articles 31 and 32. The Croatian Act limits video surveillance of public areas to public authorities, legal persons with public authority, and legal persons engaged in public service when the surveillance is mandated by law, necessary to carry out the tasks and duties of public authorities or necessary to protect human life, health, or assets.

(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, regarding Article 19 of the Croatian GDPR Implementation Act, to ensure their privacy, when Agency publishes opinions and resolutions that refer to minors, the information applicable to them are anonymized. Consent is required for children under 16 years old (Article 19 Croatian GDPR Implementation Act). That applies to children who reside in the Republic of Croatia. A violation of Article 19 of the Croatian Act is a violation a GDPR Article 8 and is subject to sanctions under GDPR Article 83.

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

No, there are no other vulnerable individuals identified in Croatian national legislation.

4.1.4 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?

There are no special provisions in Croatian GDPR Implementation Act that would apply to deceased individuals. However, the courts will honour the wishes of surviving family members and will not allow the personal data of deceased individuals to be used against their will.

[63] https://www.babic-partners.hr/wp-content/uploads/2019/02/Croatian-implementation-of-GDPR.pdf

4.1.5 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 further provisions, requirements or procedures regarding general accountability are introduced in Croatian national regulation.

(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?

No, there are no special requirements regarding the impact assessments.

4.2 Commercialization of data

4.2.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
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")	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807	Hard law	A "regulation" is a binding legislative act. It must be applied in its entirety across the EU. Therefore, in force by itself-
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")	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770	Hard law	By 1 July 2021 Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from 1 January 2022.
Zakon o provedbi Opće uredbe o zaštiti podataka	https://translate.google.com/translate?hl=en	Hard law	Implementation of GDPR in Croatia

(Implementation Act of the EU General Data Protection Regulation) (25 May 2018)	&sl=hr&u=https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html&prev=search		
The Copyright And Related Rights Act	https://www.dziv.hr/files/file/eng/zakon_autor_ENG.pdf	Hard law	Croatian legislation creating copyright rights
Zakon o zaštiti potrošača (Consumer Protection Act)	http://pak.hr/cke/propisi,%20zakoni/en/ConsumerProtectionAct/Consumer.pdf	Hard law	Croatian legislation regarding consumer protection in general

Main regulatory tools addressing data commercialization in Croatia.

4.2.2 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)? Do you know if these practices are routinely performed? Does your country have any specific regulation on the remuneration of data subjects if profit is made out of their data? Do you have any particular national regulation on the secondary use of data? Do you have any specific protection for metadata or non-personal data in your country?

All regulation is in line with GDPR. See please here: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm. In addition, concerning metadata, there are several sources of law which apply to the surveillance of communications, including

- Constitution of the Republic of Croatia,[64]
- Electronic Communications Act (ECA),[65]
- Criminal Procedure Act (CPA),[66]
- Act on Security-Intelligence System of the Republic of Croatia (ASIS),[67]
- Police Duties and Power Act (PDPA),[68]

[64] *Ustav Republike Hrvatske*, Official Gazette of the Republic of Croatia, no. 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014.
[65] *Zakon o elektroničkim komunikacijama*, Official Gazette of the Republic of Croatia, no. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017.
[66] *Zakon o kaznenom postupku,* Official Gazette of the Republic of Croatia, no. 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017.
[67] *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske,* Official Gazette of the Republic of Croatia, no. 79/2006, 105/2006.
[68] *Zakon o policijskim poslovima i ovlastima*, Official Gazette of the Republic of Croatia, no. 76/2009, 92/2014.

- Regulation on national security requirements of the Republic of Croatia for individuals and legal entities in telecommunications (NSR),[69]
- Criminal Code.[70]

The prerequisites for the surveillance of electronic communications differ between repressive criminal law, preventive police authority and intelligence.

In Croatia, coercive powers in the field of criminal procedural law are delegated to state attorneys and to the police for interception of electronic communications[71].

Pursuant to Article 33(3) of the ASIS, measures of secret information gathering include secret surveillance of telecommunications services, activity and traffic, namely:

a) Secret surveillance of communication content,

b) Secret surveillance of telecommunication traffic data,

c) Secret surveillance of the location of the user,

d) Secret surveillance of international telecommunications.

Surveillance in the field of police duties and powers

The Police are not empowered to conduct the interception of content data in the exercise of their duties and competences. They can only do so in the course of criminal proceedings, upon request and in accordance with the instructions given by the State Attorney and the courts.

Article 68 of the PDPA empowers the police to request analysis of "identity, duration and frequency of communications with specified communication addresses", (2) determination of "the location of communication devices" as well as location of "users of communication devices", as well as (3) "identification marks of communication devices". This power might be used for the purpose of (1) preventing and detecting criminal offences prosecuted ex officio and their perpetrators, (2) prevention of danger and violence, as well as (3) searching for persons and objects.

Application of Article 68 PDPA does not require judicial authorization. Instead, it is based on the written approval of the Chief of the Criminal Police Administration or of the Chief of the National Police Office for the Suppression of Corruption and Organized Crime or of the Chief of Police Administration or by their replacement in case of absence.

In exceptional circumstances, namely when it is necessary to prevent immediate danger or violence or for the purpose of an urgent search for persons, the authorization may be given orally, but must be confirmed in writing within 24 hours of the oral approval.

Finally, application of Article 68 PDPA is also subject to the principle of subsidiarity. Namely, this measure should be approved only on the basis of facts from which it is

[69] *Uredba o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama*, Official Gazette of the Republic of Croatia, no. 64/2008, 76/2013.

[70] *Kazneni zakon,* Official Gazette of the Republic of Croatia, no. 25/2011, 144/2012, 56/2015, 61/2015, 101/2017.

[71] More in Jurić Marko and Roksandić Vidlička Sunčana, I. Security Architecture and the Interception of Telecommunications (Croatia), Max Planck Institute for Foreign and International Criminal Law (in preparation) 2020

apparent that other actions could not or will not be able to attain the objective of the police work or if the achievement of that objective has presented unreasonable difficulties.

4.2.3 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 my knowledge, here is no specific definition of data 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 law is among the legal sources, as mentioned above. However, to the best of my knowledge, there is no specific mechanism to determine the value of data.

4.3 Security and cybersecurity

4.3.1 General Regulatory Framework

Regulation	Link (English version if possible be)	Type of regulation (hard law, soft law…)	Brief description and scope
Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Act on cybersecurity of operators of essential services and digital service providers)	https://translate.google.com/translate?hl=en&sl=hr&u=https://www.zakon.hr/z/1041/Zakon-o-kiberneti%25C4%258Dkoj-sigurnosti-operatora-klju%25C4%258Dnih-usluga-i-davatelja-digitalnih-usluga&prev=search	Hard law	In accordance with the NIS Directive, this act provides a general harmonization frame and is applicable in following 8 sectors: Energetics, Transport, Banking, Financial Market Infrastructure, Health sector, Water supply and distribution, Digital infrastructure and Business services for state bodies
Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (Regulation on Cybersecurity of	https://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/Regulation%20on%20cybersecurity%20of%20operators%20of%20essential%20services.pdf	Hard law	Contrary to the law, this regulation brings a number of concrete technical and organizational measures that need to be implemented, as well as the method of their execution

Operators of Essential Services and Digital Service Providers)			
Ustav Republike Hrvatske (Constitution of the Republic of Croatia)	https://azop.hr/images/dokumenti/266/theconstitutionoftherepublicofcroatia.pdf	Hard law	The Croatian Constitution provides direct protection to communication privacy (Article 36 paragraph 1) and personal data (Article 37). However, these rights are not absolute, and can be restricted in accordance with general constitutional rules and principles regarding limitations of constitutional rights.
Zakon o elektroničkim komunikacijama (Electronic Communications Act – ECA)	https://mmpi.gov.hr/UserDocsImages/arhiva/ECActOG73-2008.pdf	Hard law	The ECA regulates some aspects of the institutional framework necessary to conduct surveillance (namely, the obligation for electronic communications providers to cooperate with relevant state bodies). This Act also implements the data retention obligation for communications data, which subsequently enables relevant law enforcement authorities in the sphere of criminal procedural law to gain access to such data based on the CPA.
Zakon o kaznenom postupku (Criminal	http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Procedure-Act.pdf	Hard law	On the application of the measures of procedural coercion, i.e. regarding the interference in certain fundamental

Procedure Act – CPA)			human rights or freedoms, only a court has the authority to decide on their implementation and these measures are restrictively applied following jurisprudence of the ECtHR: they must be prescribed by law, have a legitimate aim and be necessary in a democratic society. The last condition refers to the principle of proportionality, which in Croatian law is elevated to the constitutional level.
Kazneni zakon Republike Hrvatske (Croatian Criminal Code)	http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Code.pdf	Hard law	Article 143 of the Criminal Code provides protection against unauthorised audio recording and eavesdropping. Article 146 of the Criminal Code prohibits unauthorised use of personal data and Article 269 of the same Code prohibits unauthorised interception of computer data

Main regulatory tools addressing security and cybersecurity in Croatia

4.3.2 Implementation of EU Law

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

No, as far as I am aware, no particular procedures other than provisions of the Act and the Regulation on Cybersecurity of Operators of Essential Services and Digital Service Providers that transposes the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19 July 2016) into the legislation of the Republic of Croatia and ensure the implementation of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service

providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a significant impact.

(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 the legislation of the Republic of Croatia in provisions of the Act ((»Official Gazette «, No. 64/18) and the Regulation ((»Official Gazette «, No. 68/18) on Cybersecurity of Operators of Essential Services and Digital Service Providers which came into effect in 26th of July 2018.

(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, in Article 7 of the aforementioned Regulation, operators of essential services are instructed to appoint the person with the highest managing authority who shall be responsible for establishing and managing the security of essential systems. Operators of essential services are also instructed to establish the organizational structure, with formal division of duties, authorities and responsibilities, which shall ensure the appropriate security management of essential systems. According to Article 8 they must establish the system of internal oversight of the implementation of cybersecurity measures defined by the security management policy of essential systems, whereas the internal oversight tasks are to be organizationally separate from the organizational structure responsible for essential systems.

4.3.3 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?

Act on cybersecurity of operators of essential services and digital service providers regulates the obligation to notify in its Article 21. Key service operators and digital service providers are instructed to notify the competent CSIRT, without undue delay, of incidents that have a significant effect on the continuity of the services they provide. If the incident on the network and information system of the digital service provider had a significant effect on the provision of a key service, the key service operator must inform the competent CSIRT of the incident.

Act on Security-Intelligence System of the Republic of Croatia in its Article 56 instructs security and intelligence agencies to notify State Attorney's Office where the collected intelligence indicates that a criminal act which is prosecuted ex officio is being planned or committed. However, in that case it enables the Directors of security and intelligence agencies to suggest to the Chief State Attorney to postpone further actions within his/her scope of duty, if such actions might jeopardise the achievement of the objectives falling within the scope of activity of security and intelligence agencies, or endanger the safety of the employees and sources of security and intelligence agencies.

Responsibility for notification is foreseen in Article 34 of Regulation on Cybersecurity of Operators of Essential Services and Digital Service Providers. It obligates the Operators of essential services and digital service providers to, without undue delay, notify the competent CSIRT about incidents that have a significant impact on the continuity of services they provide.

4.3.4 Supervision of cybersecurity

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

There is no independent supervision mechanism for interception measures within the Criminal Procedure Act framework.

According to Article 26 of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers, supervision of the key services operator must be carried out once every two years or before the expiry of that time limit if the competent sectoral authority determines or receives information indicating that the key services operator does not fulfil its obligations under this Law. Supervision is to be carried out only after the competent sectoral authority has received information indicating that the digital service provider is not acting in accordance with the Commission Implementing Regulation and / or the provisions of this Law. Surveillance must be carried out with the support of the competent technical conformity assessment body and the competent CSIRT. In Article 29 it is stated that supervision is to be carried out by inspectors, supervisors and supervisors, in accordance with the competences arising from the regulations on the organization and scope of work of these bodies and other regulations which determine their competence.

According to Article 8 of the Regulation on Cybersecurity of Operators of Essential Services and Digital Service Providers, operators of essential services must establish the system of internal oversight of the implementation of cybersecurity measures defined by the security management policy of essential systems, whereas the internal oversight tasks are to be organizationally separate from the organizational structure responsible for essential systems.

The Operational and Technical Centre for Telecommunications Surveillance (hereinafter OTC) is authorised to supervise the work of telecommunications services providers, i.e. their fulfilment of the obligations stipulated by Security and Intelligence System Act of the Republic of Croatia, in cooperation with the bodies authorised for the application of measures of secret telecommunications surveillance in accordance with this Act and the Criminal Procedure Act. For the purpose of security and intelligence agencies and monitoring bodies, OTC conducts the activation and management of the measures of secret surveillance of telecommunications services, activities and traffic, by means of appropriate technical interface.

(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?

Yes, The Office of the National Security Council is the Croatian NSA (National Security Authority). In that sense UVNS coordinates and harmonizes the adoption and controls the implementation of information security measures and standards in the areas of Security Vetting, Physical Security, Security of Information, INFOSEC and Industrial Security (Croatian DSA) and issues clearances for individuals and legal entities for access to national, NATO and EU Classified Information. Central Registry is organized within UVNS and it is competent for the reception and

distribution of international Classified Information and for the coordination of the work of the Registry system in Croatian state authorities which receive international Classified Information. As Croatian NSA, UVNS carries out and coordinates international cooperation in the field of information security and based on the Government Decision concludes international security agreements for the protection of Classified Information on behalf of the Republic of Croatia.[72]

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

According to the Article 41 of Croatian Law on GDPR Implementation, Respondent has the right to authorize a non-profit body, organization or association established in accordance with the law, whose statute sets out goals of public interest and is actively involved in protecting the rights and freedoms of respondents with respect to the protection of his or her personal information, to file a complaint with his / her and to exercise on his behalf the rights referred to in Articles 77, 78 and 79 of the General Data Protection Regulation and the right to compensation referred to in Article 82 of the General Data Protection Regulation.

4.4 Enforcement: fines and sanctions

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

Article 143 of the Croatian Criminal Code provides protection against unauthorised audio recording and eavesdropping. Article 146 of the Criminal Code prohibits unauthorised use of personal data and Article 269 of the same Code prohibits unauthorised interception of computer data. The provisions are as following:

Article 143

Unauthorised Audio Recording and Eavesdropping

(1) Whoever audio records without authorisation another person's privately uttered words or by means of special devices eavesdrops without authorisation another person's privately uttered words that are not intended to be heard by him/her

shall be sentenced to imprisonment for a term of up to three years.

(2) The sentence referred to in paragraph 1 of this Article shall be imposed on whoever uses or makes available to a third party the recorded words referred to in paragraph 1 or whoever publicly reveals word for word the eavesdropped words referred to in paragraph 1 or their gist.

(3) If the criminal offences referred to in paragraphs 1 and 2 of this Article are committed by a public official in the performance of his/her functions or the exercise of public authority,

he/she shall be sentenced to imprisonment for a term of between six months and five years.

(4) There shall be no criminal offence if the acts referred to in paragraphs 1 and 2 of this Article are committed in the public interest or another interest prevailing over the interest to protect the privacy of the person being recorded or eavesdropped on.

[72] https://www.uvns.hr/en/scope-of-work/information-security-nsa

(5) The criminal offences referred to in paragraphs 1 and 2 of this Article shall be prosecuted upon request.

(6) The recordings and special devices used for committing the criminal offence referred to in this Article shall be seized.

Article 146

Unauthorized use of personal data

(1) Whoever, in contravention of the conditions set out in the act, collects, processes or uses personal data of physical persons

shall be sentenced to imprisonment for a term of up to one year.

(2) Whoever, in contravention of the conditions set out in the act, transfers personal data outside of the Republic of Croatia for further processing, or makes them public or in some other way available to a third party, or whoever by the act referred to in paragraph 1 of this Article acquires significant pecuniary gain for himself/herself or another or causes considerable damage

shall be sentenced to imprisonment for a term of up to three years.

(3) The sentence referred to in paragraph 2 of this Article shall be imposed on whoever commits the offence referred to in paragraph 1 of this Article against a child or on whoever, in contravention of the conditions set out in the act, collects, processes or uses personal data of physical persons on the racial or ethnic origin, political views, religious or other beliefs, trade union membership, health or sex life or the personal data of physical persons on criminal or misdemeanour proceedings.

(4) If the criminal offences referred to in paragraphs 1 through 3 of this Article is committed by a public official in the exercise of his/her authorities,

he/she shall be sentenced to imprisonment for a term of between six months and five years.

Article 269

Unauthorised interception of computer data

(1) Whoever intercepts or records without authorisation non-public transmissions of computer data, including electromagnetic emissions from a computer system, or makes available to another the data thus procured

shall be sentenced to imprisonment for a term of up to three years.

(2) A perpetrator who attempts to commit the criminal offence referred to in paragraph 1 of this Article shall be punished.

(3) The data derived from the commission of the criminal offence referred to in paragraph 1 of this Article shall be destroyed.

In addition, according to Croatian Criminal Code, Article 133, unauthorized use of personal data is punishable by a fine or imprisonment. It states that whoever, without the consent of citizens and contrary to the conditions stipulated by the law, collects, processes or uses personal data, or uses such data contrary to the statutory purpose of their collection is to be punished by a fine or by imprisonment not exceeding three years.

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

Yes, Croatian Personal Data Protection Agency imposes administrative fines for violations of the provisions of Croatian GDPR Implementation Act and the General Data Protection Regulation, in accordance with Article 83 of the General Data Protection Regulation.

Act on Cybersecurity of Operators of Essential Services and Digital Service Providers also imposes various administrative fines in Articles 42,43,44 and 45.

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

Data protection offences constitute an official offence. For example, State Attorney is the authorized prosecutor for the offence referred to in Article 50 of Croatian GDPR Implementation Act.

4.5 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?

As already mentioned, there is CESHE, or Croatian Committee on Ethics in Science and Higher Education. In addition, every University, Medical hospital etc. has its own ethics committee that is responsible for approval of research including the usage of data. Reviews are preformed regularly and the anonymity of data, and access to databases is strictly controlled if it is in accordance with the GDPR.

(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?

In Croatia, research bodies, for example University of Zagreb abide by the European Code of Conduct for Research Integrity .

The Technical Assessment Body for the Business Services sector for government bodies for all services is the Office for Security of Information Systems, except for the field within the competence of the central government authority responsible for science and education, University Computing Center (Heart) or Croatia academic and research networks - CARNET, for which the technical conformity assessment body is the Croatian Academic and Research Network - CARNET.

Research Ethics Committees in general deal with legal and ethical compliance about data protection in research, each in his own competence.

(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?

As Croatia is EU member state the following Regulation is applicable: Commission Delegated Regulation (EU) 2017/2268 of 26 September 2017 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items in order to ensure full compliance with international security obligations as the changes to the control lists were adopted by the international non-proliferation regimes and export control arrangements in 2016. Commission Delegated Regulation entered into force on 16 December 2017.

Regulation (EC) No 428/2009 empowers the Commission to update the list of dual-use items set out in Annex I as well as Annexes IIa to IIg and Annex IV by means of delegated acts, in conformity with the relevant obligations and commitments, and any modifications thereto, that Member States have accepted as members of the international non-proliferation regimes and export control arrangements, or by ratification of relevant international treaties.

The changes to the control lists have been taken within the framework of the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group and the Wassenaar arrangement.[73]

As regards industrial espionage, in most serious cases also Articles 347 (Disclosure of Secret Information) and 348 (Espionage) of the Croatian Criminal Code can apply.

Disclosure of Secret Information Article 347

(1) Whoever makes available to an unauthorised person secret information confided to him/her shall be sentenced to imprisonment for a term of between six months and five years.

(2) Whoever obtains a secret piece of information with the aim that he/she or an unauthorised person uses it without authorisation, or whoever makes available to another such a piece of information which has come into his/her possession by accident shall be sentenced to imprisonment for a term of up to three years.

(3) Whoever commits the offence referred to in paragraph 1 or 2 of this Article out of love of gain

shall be sentenced to imprisonment for a term of between one and ten years.

(4) Whoever commits the criminal offence referred to in paragraph 1 or 2 of this Article in a state of war or immediate threat of war

shall be sentenced to imprisonment for a term of between three and twelve years.

(5) Whoever commits the criminal offence referred to in paragraph 1 of this Article by negligence shall be sentenced to imprisonment for a term of up to three years.

Espionage Article 348

(1) Whoever makes available to a foreign state, foreign organisation, foreign legal person or a person working for them secret intelligence confided to him/her or which he/she has unlawfully obtained shall be sentenced to imprisonment for a term of between one and ten years.

[73] http://gd.mvep.hr/hr/kontrola-izvoza/export-control/dual-use-items/overview/

(2) Whoever collects secret intelligence without authorisation with the aim of making it available to a foreign state, foreign organisation, foreign legal person or a person working for them

shall be sentenced to imprisonment for a term of between six months and five years.

(3) Whoever organises for a foreign state or organisation an intelligence service in the territory of the Republic of Croatia, or joins a foreign intelligence service acting against the interests of the Republic of Croatia, or assists it in its work

shall be sentenced to imprisonment for a term of between one and ten years.

(4) Whoever commits the criminal offence referred to in paragraph 1 or 3 of this Article in times of war or armed conflict in which the Republic of Croatia participates shall be sentenced to imprisonment for a term of at least five years.

(5) Whoever commits the criminal offence referred to in paragraph 2 of this Article in times of war or armed conflict in which the Republic of Croatia participates shall be sentenced to imprisonment for a term of between three and fifteen years.

5 Republic of Cyprus

Nikitas Hatzimihail, Elvira Pallikarou (University of Cyprus)

5.1 Informed consent

5.1.1 General Regulatory Framework

Regulation	Link (English version if possible)	Type of regulation (hard law, soft law…)	Brief description and scope
Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος [Ν.125(Ι)/2018]	Original: http://www.cylaw.org/nomoi/enop/non-ind/2018_1_125/full.html English: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/2B53605103DCE4A4C225826300362211	Hard law	Law 125(I)/2018 aligns national legal framework with the GDPR, as it relates to areas left for Member States to provide for.