(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.

	*Please note that this version is an unofficial translation of the relevant law 125(I)/2018 by the Office of the Commissioner for Personal Data Protection.		
Ο περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος [Ν. 112(Ι)/2004) **(Σχετικό είναι το Μέρος 14- Ασφάλεια και Ακεραιότητα Δικτύων και Υπηρεσιών & Ασφάλεια, Απόρρητο και Προστασία Δεδομένων)**	Original: http://www.cylaw.org/nomoi/enop/non-ind/2004_1_112/full.html	Hard Law	Section 14 of Law 112(I)/2014 provides the framework for network safety, privacy and data protection. The scope is to protect individual's right to private life and confidentiality, while using the relevant online services in the field of online communication.
Κυρωτικός του Τροποποιητικού Πρωτοκόλλου στη Σύμβαση για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/F513F2D48F073174C22586CD0041728D/$file/6(%CE%99%CE%99%CE%99)-2020.pdf?openelement	Hard Law	Ratification of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

του 1981 Νόμος [N. 6(III)/2020]			
Ο περί του Πρόσθετου Πρωτοκόλλου στη Σύμβαση για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του 1981 (Κυρωτικός) Νόμος [N.30(III)/2003]	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/F513F2D48F073174C22586CD0041728D/$file/30(%CE%99II)-2003.pdf?openelement	Hard Law	Ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows (ETS 181).
Ο περί της Σύμβασης για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (Κυρωτικός) Νόμος [N.28(III)/2001]	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/F513F2D48F073174C22586CD0041728D/$file/28(III)-2001_el.pdf?openelement	Hard Law	Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108).
Γνώμη 1/2018 της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα προς Όλες τις Συντεχνίες Αναφορικά με	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%93%CE%BD%CF%8E%CE%BC%CE%	Soft Law (Opinion)	Opinion of the Cypriot Commissioner for Personal Data Protection on the publication by the employer of the employee's salary and contribution to their Unions.

την Κοινοποίηση από τους Εργοδότες Ονομαστικής Κατάστασης με τον Μισθό και το Ποσό της Εισφοράς που Αποκόπτεται από του Υπαλλήλους – Μέλη Συντεχνιών	B7%201-2018%20%CF%80%CF%81%CE%BF%CF%82%20%CF%83%CF%85%CE%BD%CF%84%CE%B5%CF%87%CE%BD%CE%AF%CE%B5%CF%82.pdf?openelement		
Γνώμη 2/2018 που εκδίδεται από την Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα βάσει του Άρθρου 58(3)(β) του Γενικού Κανονισμού για τη Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) για τη Βιντεο-παρακολούθηση στο χώρο εργασίας και τη χρήση βιομετρικών συστημάτων.	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%93%CE%BD%CF%8E%CE%BC%CE%B7%202-2018%20%CE%B3%CE%B9%CE%B1%20%CE%9A%CE%9A%CE%92%CE%A0%20%CE%BA%CE%B1%CE%B9%20%CE%B2%CE%B9%CE%BF%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%AC%20%CF%83%CF%84%CE%BF%20%CF%87%CF%8E%CF%81%CE%BF%20%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%C	Soft Law (Opinion)	Opinion of the Cypriot Commissioner for Personal Data Protection on CCTVs at working environments and use of biometrics.

	E%B1%CF%82.pdf?openelement		
Γνώμη 1/2019 της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αναφορικά με την πρόσβαση στον λογαριασμό ηλεκτρονικού ταχυδρομείου των εργοδοτουμένων/ πρώην εργοδοτουμένων και την επεξεργασία προσωπικών δεδομένων που είναι αποθηκευμένα σε αυτά.	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/2019-access%20to%20email%20accounts%20by%20the%20employer.pdf?openelement	Soft Law (Opinion)	Opinion of the Cypriot Commissioner for Personal Data Protection on the access to the email addresses of current employees and former employees and processing of personal data stored in these email addresses.
Ερμηνεία του Άρθρου 10 του Γενικού Κανονισμού για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679)	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%95%CF%81%CE%BC%CE%B7%CE%BD%CE%B5%CE%AF%CE%B1%20%CF%84%CE%BF%CF%85%20%CE%AC%CF%81%CE%B8%CF%81%CE%BF%CF%85%2010%20%CF%84%CE%BF%CF%85%20%CE%93%CE%9A%CE%	Soft Law (Opinion)	Opinion of the Cypriot Commissioner for Personal Data Protection on the interpretation of article 10 of the GDPR, specifically regarding personal data on criminal convictions and offences.

	A0%CE%94.pdf?openelement		
Γνώμη 1/2020 της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα αναφορικά με την Επιτήρηση των εξ' αποστάσεως/ διαδικτυακών εξετάσεων από ιδρύματα ανώτερης εκπαίδευσης	Original: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%93%CE%BD%CF%8E%CE%BC%CE%B7%201-2020%20-%20%CE%95%CF%80%CE%B9%CF%84%CE%AE%CF%81%CE%B7%CF%83%CE%B7%20%CF%84%CF%89%CE%BD%20%CE%B5%CE%BE%20%CE%B1%CF%80%CE%BF%CF%83%CF%84%CE%AC%CF%83%CE%B5%CF%89%CF%82%20%CE%B5%CE%BE%CE%B5%CF%84%CE%AC%CF%83%CE%B5%CF%89%CE%BD.pdf?openelement	Soft Law (Opinion)	Opinion of the Cypriot Commissioner for Personal Data Protection on the regulation of distance examinations or online exams by institutions of higher education.
Οδηγίες για την αποστολή μηνυμάτων και διενέργεια κλήσεων πολιτικού περιεχομένου / προώθησης υποψηφιοτήτων (2021)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%A0%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AE%20%CE%B5%CF%80%CE%B9%CE	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the promotion of candidacy via calls and circulation of sms of political content.

	%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%AF%CE%B1%20-%20%CF%80%CF%81%CE%BF%CF%8E%CE%B8%CE%B7%CF%83%CE%B7%20%CF%85%CF%80%CE%BF%CF%88%CE%B7%CF%86%CE%B9%CE%BF%CF%84%CE%AE%CF%84%CF%89%CE%BD%202021.pdf?openelement		
Οδηγία για το χρονικό διάστημα διατήρησης δεδομένων που αφορούν στην υγεία (2018)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%9F%CE%B4%CE%B7%CE%B3%CE%AF%CE%B1%20%CE%B3%CE%B9%CE%B1%20%CF%87%CF%81%CF%8C%CE%BD%CE%BF%20%CE%B4%CE%B9%CE%B1%CF%84%CE%AE%CF%81%CE%B7%CF%83%CE%B7%CF%82%20%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD%20%CF%85%CE%B3%CE%B5%CE%AF%CE%B1%CF%82%2	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the overall time that personal data concerning health may be kept.

	02018.pdf?openelement		
Οδηγία για την άσκηση του δικαιώματος πρόσβασης από τους υπαλλήλους στο Δημόσιο Τομέα (Αρ. 4/2017)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%9F%CE%B4%CE%B7%CE%B3%CE%AF%CE%B5%CF%82%204-2017%20%CE%B3%CE%B9%CE%B1%20%CE%B4%CE%B9%CE%BA%CE%B1%CE%AF%CF%89%CE%BC%CE%B1%20%CF%80%CF%81%CF%8C%CF%83%CE%B2%CE%B1%CF%83%CE%B7%CF%82%20%CF%85%CF%80%CE%B1%CE%BB%CE%BB%CE%B7%CE%BB%CF%8E%CE%BD%20%CF%83%CF%84%CE%B7%20%CE%B4%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%B1%20%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%AF%CE%B1.pdf?openelement	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the right of employees or potential employees to the public sector to have access to information regarding their evaluation.
Οδηγία για την πραγματοποίηση πολιτικής επικοινωνίας μέσω τηλεφωνικών	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%9F%CE%B4%CE%B	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the making of politically related calls, regarding upcoming elections.

κλήσεων (Αρ.3/2017)	7%CE%B3%CE%AF%CE%B5%CF%82%203-2017%20%CE%B3%CE%B9%CE%B1%20%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AD%CF%82%20%CE%B4%CE%B9%CE%B1%CF%86%CE%B7%CE%BC%CE%AF%CF%83%CE%B5%CE%B9%CF%82.pdf?openelement		
Οδηγία προς Τραπεζικούς Οργανισμούς για τον καθορισμό του χρονικού διαστήματος διατήρησης δεδομένων (Οδηγίες Αρ.1/2017 και Αρ.2/2017)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%9F%CE%B4%CE%B7%CE%B3%CE%AF%CE%B5%CF%82%20%CF%80%CF%81%CE%BF%CF%82%20%CE%91%CE%A0%CE%99%20%CE%B3%CE%B9%CE%B1%20%CF%87%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C%20%CE%B4%CE%B9%CE%AC%CF%83%CF%84%CE%B7%CE%BC%CE%B1%20%CE%B4%CE%B9%CE%B1%CF%84%CE%AE%CF%81%CE%B7%CF%83%CE%B7%	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the overall time that personal data may be kept by a bank.

	CF%82.pdf?openelement		
Βιντεο-παρακολούθηση σε δημόσιους χώρους από Τοπικές Αρχές (Οδηγία του 2016)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/CCTV%20local%20auth%202016.pdf?openelement	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on CCTV's in public spaces.
Οδηγία για απ' ευθείας εμπορική προώθηση πώλησης αγαθών ή παροχής υπηρεσιών με ηλεκτρονικά μέσα (Οδηγία του 2011)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/Direct%20marketing%20directions.pdf?openelement	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on
Χρήση του Διαδικτύου και των κινητών τηλεφώνων (Οδηγία του 2007)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/Internet&MobilePhoneUse.pdf?openelement	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on direct marketing using the email.
Οδηγία Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για την Επεξεργασία Προσωπικών Δεδομένων στον Τομέα των Εργασιακών Σχέσεων.	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/Directive-Employment_el(1).pdf?openelement	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the collection and processing of the personal data of employees by the employer.

Βίντεο-παρακολούθηση (Οδηγία του 2004)	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/Directive-VideoSurveillance_el.pdf?openelement	Soft Law (Guidelines)	Guidelines given by the Cypriot Commissioner for Personal Data Protection on the placement and use of CCTVs.

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

(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?

The legal framework in force regarding the protection of personal correspondence is the following:

Ο περί της Προστασίας του Απορρήτου της Ιδιωτικής Επικοινωνίας (Παρακολούθηση Συνδιαλέξεων και Πρόσβαση σε Καταγεγραμμένο Περιεχόμενο Ιδιωτικής Επικοινωνίας) Νόμος [92(I)/1996].

The above-mentioned legislation creates several criminal offences regarding the deliberate monitoring or in any way retaining access to any form of personal correspondence without the consent of the third person, imposing the maximum fine of 100.000 euro and/or up to 10 years imprisonment.

In addition, the Cyprus Constitution provides protection to personal and family life, with minimal and legally provided for exceptions regarding public safety, public health and several analogous reasons.

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

Law 125(I)/2018 (as referred to above) creates at article 33(4) an idionymous offence in cases where the controller or the processor commit a crime provided for at article 33(1) Poland GDPR and the above-mentioned legislation and affects at the same time the national security of the Republic of Cyprus. In such cases there is a fine of up to 50.000 euro and/or up to 5 years of imprisonment.

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

Office of the Commissioner for Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument	According to article 19 of Law 125(I)/2018, the commissioner is being appointed by the Council of Ministers and ought to meet the requirements in place for appointment as a Supreme Court Judge. There is a 6 years' service and the commissioner may not be suspended except in cases of mental or physical incapacity. Therefore, although the commissioner is being appointed by the government, she is free to exercise her duties as she thinks best given that she may not be suspended based on their approach to several issues. She, furthermore, does not accept any directions from other	14 people of which 5 have secretarial duties.	High.	Provides guidelines on several queries and matters of general interest regarding the application of the GDPR throughout the year.

		bodies of power.			

Information regarding Data Protection Authorities, Cyprus.

(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.?

There is no specific definition of the terms "data processing for research purposes" and "research in public interest".

(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?

Law 125(I)/18 refers under article 31 to, amongst other, scientific and historical research as well as to research in the public interest and states that processing of data by a controller or a processor for such purposes may not constitute processing of data able to create legal rights of the data subject.

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

According to article 9 of the law 125(I)/18, processing of genetic and biometric data for the purposes of health and life insurance is forbidden. In addition, in cases where the processing of genetic and biometric data takes place with the consent of the data subject, further processing would require the separate and specific consent of the data subject.

(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.)?

There are codes of practice in the form of secondary legislation under article 18 of the law N.150(I)/2001 regulating the National Bioethics Committee.

The objective of the Code of Practice of the Review Bioethics Committees (RBCs) is to contribute to the development of a proper methodology for the bioethical and deontological review of research in Cyprus. The Code is intended to serve as the RBC Regulations regarding scientific research in Cyprus and to establish a credible and valid level of assurance of qualitative bioethical review.

It is based on a close examination of the requirements for review as established in international guidelines and codes, such as the Declaration of Helsinki, the International Ethical Guidelines for Biomedical Research Involving Human Subjects and Good Clinical Practice Guidelines of the World Health Organization (WHO).

For research to be approved by the committee there is specific and detailed documentation to be filed which includes reference to the processing, usage and generally the protection of the personal data that will be collected for the purposes of the study. The committee ought to assure that the dignity, safety, wellbeing and generally the rights of the potential subjects of research are well protected.

(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 specific definition provided under the relevant national legislation for the term **"statistical purposes"**. However, Law 125(I)/18 refers under article 31 to, amongst other, research for statistical purposes and states that processing of data by a controller or a processor for such purposes may not constitute processing of data able to create legal rights of the data subject.

(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 further references are founded in national legislation and therefore the basic provisions of the GDPR are being followed.

5.1.2 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.)

No particularities have been spotted.

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

The meaning of the term "consent" as given in article 2 of the law 125(I)/18 is the same as the one given in article 4 of the GDPR.

Special requirements regarding informed consent are in place regarding minors at article 8 of the law 125(I)/18, providing that processing of his/her data is legal if his/her consent is given except in cases that he/she is under the age of 14 where the consent of the person that has the custody is required.

Further specific reference to the consent of the data subject is made in article 9 of the law 125(I)/18 regarding the processing of genetic and biometric data, providing that such processing shall be legal only if based on the consent of the data subject while further processing would require further specific consent.

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

No special requirements have been spotted.

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

No special requirements are in place to exercise data subject's rights.

5.1.3 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)?

According to article 5 of law 125(I)/18, the processing of personal data by the Courts or the House of Representatives within the limit of their powers under is allowed, including the publication of a court decision.

Furthermore, as has already been mentioned above, according to article 9 of the law 125(I)/18, processing of genetic and biometric data for the purposes of health and life insurance is forbidden. In addition, in cases where the processing of genetic and biometric data takes place with the consent of the data subject, further processing would require the separate and specific consent of the data subject.

Article 29 of the law 125(I)/18 is also relevant. It constitutes a transfer of article 85 of the GDPR to the national law and provides that processing of personal data, personal data of special categories or personal data related to criminal records which takes place for journalistic or academic purposes, art or literature, is legal given that the principle of proportionality is fulfilled, and the human rights of the subjects are reserved.

It should also be mentioned that every reference to a person under the national law includes the legal person.

Provisions regarding the protection of sensitive personal data are also to be found in the legal framework establishing the national health system of Cyprus. More specifically, section X of law 89(I)/2001 provides for the protection of sensitive personal data during processing either from the state or from the individual health providers.

In general, legislations that need to include provisions for the protection of personal data, make reference to the umbrella act 125(I)/2018 which is preferred as it ensures unity in the approach.

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

According to article 8 of law 125(I)/18, for collecting and processing the personal data of a minor his/her consent shall be obtained in cases where he/she is over the age of 14. In other cases, where the minor is under the age of 14, the consent of the person that has the custody shall be obtained instead.

Consent of a minor can be valid if he/she is over the age of 14.

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

There are no other categories of vulnerable individuals under national law.

5.1.4 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?

Law 141(I)/2002 which includes provisions regarding the civil registry, provides at sections III and IV that a registry of deaths is being kept in each district. The information therein may be altered or corrected following a specific procedure (articles 40-44), however, there is no provision for the erasure of such data as “a right to be forgotten”.

5.1.5 Accountability and Data Protection Impact Assessment

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

Law 125(I)/18 specifically provides at article 15 that, despite the individual provisions of any other act on the protection of personal data, the data protection officer ought to fulfil his/her obligations for privacy and confidentiality.

(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?

Law 125(I)/18, includes several references to the requirements for data protection impact assessment:

- Article 10 provides that in cases of intersectional registries between governmental authorities, when it relates to special categories of personal data or personal data related to criminal records or the ID number of a person is going to be used, a data protection impact assessment shall be conducted, after prior consultation with the commissioner for the protection of personal data.

- Article 11, making use of article's 23 of the GDPR leeway, provides that a processor may restrict the scope of the obligations and rights provided for in Articles 12, 18, 19 and 20 of the GDPR, in so far as there is respect to fundamental rights and freedoms of the data subject and necessity and proportionality are fulfilled. For the above shrinkage of the subject's rights, a data protection impact assessment shall be conducted, following prior consultation with the commissioner for the protection of personal data. In such assessment, the details provided for in articles 23(2) and 35(7) of the GDPR shall be included as well as a description of the technical and organisational measures as provided for in articles 24, 25, 28 and 32 of the GDPR.

- Article 11 provides that a processor may refer from notifying the data subject for a personal data breach for the reasons described in article 23(1) of the GDPR. In such case, the processor must conduct a data protection impact assessment, after prior consultation with the commissioner for the protection of personal data. Such assessment may include the details provided for in articles 23(2) and 35(7) of the GDPR.

- Article 13 poses the obligation of conducting a data protection impact assessment as well as prior consultation with the commissioner for personal data protection before the enforcement of an act or secondary legislation which relate to personal data processing. There is an exception in cases where the commissioner believes that the assessment which took place during the drafting of the legislation is enough. It shall also be mentioned that according to article 33(1)(στ) of law 125(I)/18, a processor that fails to conduct such an assessment under article 13 commits a criminal offence and shall be under a fine of up to 10.000 euro and/or up to 3 years of imprisonment.

- Article 18 provides for the transfer of special categories of personal data to a third country or an international organisation. In these cases, a data protection impact assessment as well as prior consultation with the commissioner is required. In such assessment, the details provided for in article 35(7) of the GDPR shall be included as well as a description of the technical and organisational measures as provided for in articles 24, 25, 28 and 32 of the GDPR.

5.2 Commercialization of data

5.2.1 General Regulatory Framework

Regulation	Link (English version if possible be)	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 [N.125(I)/2018] **See specifically Article 33(1)(ια).**	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 *Please note that this version is an unofficial translation of the relevant law 125(I)/2018 by the Office of the Commissioner for Personal Data Protection.	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.

Main regulatory tools addressing data commercialization in Cyprus.

5.2.2 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?

There is no legal framework governing particularly this field. Therefore, the legality or not of such a contract would be regarded under the general rules of contract law. However, one should have in mind that article 33(1)(ια) of law 125(I)/18 which creates the criminal offences deriving from actions against the provisions of the act reads as follows in liberal translation:

"A criminal offence is being committed by a person who, without authorization, intervenes in any way in a personal data archiving system or becomes aware of such data or removes, alters, damages, destroys, processes, exploits in any way, transmits, announces, makes accessible to non-entitled persons or allows such persons to become aware of such data, either for profit or not."

Such person is under a fine of up to 30.000 euro and/or imprisonment up to 3 years.

There is, however, no case law on this matter, therefore there is no judicial interpretation of the relevant legal provision.

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

There are no relevant records.

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

There is no legal framework governing particularly this field.

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

There is no legal framework governing particularly this field.

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

There are specific references to metadata in the following acts that derive from EU obligations:

- Ο περί της Περαιτέρω Χρήσης Πληροφοριών του Δημοσίου Τομέα Νόμος (N.205(I)/2015).[74]

  The act constitutes the harmonization of internal law with Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information and Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

  Article 9 provides that public sector bodies shall make their documents available in any pre-existing format or language, and, where possible and appropriate, in open and machine-readable format together with their metadata at www.data.gov.cy. Both the format and the metadata should, in so far as possible, comply with formal open standards.

  For the protection of such data there is reference to the national legal framework regarding the protection of personal data (article 3).
- Ο περί της Δημιουργίας Υποδομής Χωρικών Δεδομένων (INSPIRE) Νόμος (N.43(I)/2010).[75]

[74] http://www.cylaw.org/nomoi/enop/non-ind/2015_1_205/full.html
[75] http://www.cylaw.org/nomoi/enop/non-ind/2010_1_43/full.html

The act constitutes the harmonization of internal law with Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

The act contains several provisions regarding the handling of metadata regarding spatial information (articles 8, 9, 12).

For the protection of such data there is reference to the national legal framework regarding the protection of personal data (article 14(4)).

5.2.3 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?

Cyprus does not provide any formal classification of data but only determines "personal data" by borrowing the definition given in the GDPR.

(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?

The legal framework in Cyprus for the protection of intellectual property, and therefore assuring data and copyright protection, is law N.59/1976.

There is no specified mechanism to determine the value of data. However, it could be said that the legislature attempted a pre-evaluation of such data when deciding the corresponding to each breach fines and imprisonment time. For example, selling or renting of a copy of a product protected under intellectual property provisions constitutes a crime under N.59/1976 article 14(1) and conviction leads to a fine of up to 80.000 euro and/or imprisonment of up to 3 years. At the same time, person that knowingly presents or allows the presentation of a scientific or musical piece protected under intellectual property legislation commits a crime under N.59/1976 article 14(3) and conviction leads to a fine of up to 30.000 pounds and/or imprisonment of up to 3 years.

In addition, law N.59/1976 includes Appendix 1 which provides different times during which each type of data/intellectual property is under protection. For example, movies would be protected for 70 years from the death of the last alive creator of the movie while a broadcast would be protected for 50 years from the rediffusion.

Regarding the protection of personal data, law N.59/1976 makes reference, at article 7IK, to the umbrella act 125(I)/2018 which is preferred as it ensures unity in the approach.

5.3 Security and cybersecurity

5.3.1 General Regulatory Framework

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

Ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος (Ν.17(Ι)/2018)	Original: http://www.cylaw.org/nomoi/enop/non-ind/2018_1_17/full.html	Hard law	Constitutes a transfer in the national law of 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.
Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφαση του 2020 (Κ.Δ.Π. 408/2020)	Original: https://dsa.cy/wp-content/uploads/Decision-408-2020.pdf	Soft law (order published by the DSA under N.17(I)/18)	Directions regarding the Cyber Security of 5G services.
Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Εγγραφή Παροχέων Ψηφιακών Υπηρεσιών) Απόφαση του 2020 (Κ.Δ.Π. 403/2020)	Original: https://dsa.cy/wp-content/uploads/Decision-403-2020.pdf	Soft law (order published by the DSA under N.17(I)/18)	Directions regarding the registration of digital service providers.
Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών)	Original: https://dsa.cy/wp-content/uploads/Decision-389-2020.pdf	Soft law (order published by the DSA under N.17(I)/18)	Directions regarding the security measures taken by the operators of essential services or digital service providers.

Απόφαση του 2020 (Κ.Δ.Π. 389/2020)			
Η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019)	Original: https://dsa.cy/wp-content/uploads/Decision-218-2019.pdf	Soft law (order published by the DSA under N.17(I)/18)	Directions regarding incident notification.

Main regulatory tools addressing security and cybersecurity in Cyprus

Please note that there are no particular procedures regarding technical and organisational measures to protect personal data in national legislation, except the general provision in law 125(I)/18 which merely reflects the corresponding GDPR provision

5.3.2 Implementation of EU Law

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

There are no particular procedures in Cyprus law other than the framework implemented for the purposes of incorporation of the NIS directive provisions.

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

NIS directive has been implemented in Cyprus by act 17(I)/2018 as described in the table above. A national competent authority has been appointed which is responsible for the implementation of the relevant legislation and the materialization of national strategy for cybersecurity. In addition, the National Digital Security Authority (DSA) has been created under article 3(3) of the above-mentioned act, to the aid of the responsibilities of the national competent authority.[76]

(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?

There are no particular procedures specifying the technical and organisational measures that need to be in place in order to protect personal data in national legislation, but only some general provision in law 125(I)/18 which merely reflects the corresponding GDPR provision.

It should, however, also be mentioned that one of the DSA's responsibilities under law 17(I)/2018, article 13(ιη) is to assure that the operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

Under this responsibility, the DSA have issued decision n. 389/2020 as mentioned in the table above, which regulates the security measures taken by the operators of essential services or digital service providers. At paragraph 6, the DSA makes a reference to the responsibilities of the operator, of which the most important is the conducting of annual

[76] Information about the National Digital Security Authority can be found here < https://dsa.cy/en/>.

risk assessment, business continuity plans and disaster recovery plans. This decision also offers at Appendix 3 a security measures framework to be followed by the operators, divided in 3 sections, namely Prepare, Protect & Detect and Respond.

5.3.3 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?

Article 33(1)(δ) of N.125(I)/18 provides that in cases where the processor does not notify in due time the controller about a data breach according to article 33(2) of the GDPR commits a crime which in case of conviction leads to a fine of up to 30.000 euro and/or up to 3 years of imprisonment.

As it relates to national legislation implementing NIS directive, it should be mentioned that amongst other responsibilities of the DSA under article 13(ιστ) of N.17(I)/18 is to cooperate with the Commissioner for Personal Data Protection to incidents leading to breaches of personal data.

Under this responsibility, the DSA have issued decision n. 218/2019 as mentioned in the table above, which regulates the notification of the DSA by the operators regarding cyber security incidents. This framework offers guidance at paragraph 4(2) and Appendix 1 over the evaluation of the importance of the incident, such as the number of users that are affected, the duration of the incident, the effect of the incident to health, security, national security, economy, social and political wellbeing as well as to the environment. The procedure to be followed in notifying the DSA is also described therein.

5.3.4 Supervision of cybersecurity

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

Regarding Cyber Security, it could be said that such a supervisory body is the DSA. Under article 13(κε) of N.17(I)/18, the DSA may give an administrative fine to any person that acts in breach of the provisions of the specific act or to any orders issued by the DSA regarding cyber security and protection of data. Such administrative measures, according to article 30, is a fine of up to 8.500 euro depending on the importance of the breach.

(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?

This is the National Digital Security Authority established under L. 17(I)/18 as has been already mentioned above. Its competences and responsibilities are described in article 13 and in liberal translation are the following:

The Authority

i. Advises the Minister of Transport, Communications and Works on issues regarding digital security in the Republic of Cyprus.

ii. Applies the general framework of national strategy according to article 12, on issues regarding security of network and information systems.

iii. Constitutes the national point of contact for the security of network and information systems.

iv. Exercises, as a point of contact, a liaison function to ensure cross-border cooperation with the relevant authorities in other Member States as well as with the Cooperation Group referred to in Article 11 of Directive (EU) 2016/1148 and the CSIRTs network referred to in Article 12 of Directive (EU) 2016/1148.

v. Consults and cooperates with the relevant national law enforcement authorities and the Commissioner for the Protection of Personal Data.

vi. Submits, until the 9th of August 2018 and then yearly, as a point of contact, to the Cooperation Group referred to in Article 11 of Directive (EU) 2016/1148, a summary report on the notifications received, including the number of notifications and the nature of notified incidents, according to the relevant provisions of Directive (EU) 2016/1148.

vii. Ensures that has adequate resources to carry out, in an effective and efficient manner, the tasks included in Annex I, point 2 of Directive (2016/1148).

viii. Ensures effective, efficient, and secure cooperation of the national CSIRT in the CSIRT network referred to in Article 12 of Directive (EU) 2016/1148.

ix. Requests, where thinks necessary, the assistance of ENISA and of other European and international organisations in developing national CSIRT.

x. Receives incident notifications at a national level as well as the notifications submitted to the DSA from competent authorities of other Member States.

xi. Informs the Commission about the remit, as well as the main elements of the incident-handling process, of the national CSIRTs.

xii. Supervises the national CSIRT, the governmental CSIRT, the academic CSIRT, and/or other sector-specific CSIRT in the Republic.

xiii. Ensures that the national CSIRT has access to an appropriate, secure, and resilient communication and information infrastructure at national level.

xiv. Identifies, through its decisions issued according to N.17(I)/18, for each sector and subsector referred to in Annex II of Directive (EU) 2016/1148, the operators of essential services with an establishment in the Republic.

xv. Reviews and, where appropriate, updates the list of identified operators of essential services, on a regular basis and at least every two years after 9 May 2018. Also updates the list of critical information infrastructure operators at least every two years.

xvi. Works in close cooperation with the Commissioner for the Protection of Personal Data when addressing incidents resulting in personal data breaches.

xvii. Assesses the compliance of operators of essential services with their obligations and the effects thereof on the security of network and information systems, as well as the compliance of critical information infrastructure operators according to the relevant legislation.

xviii. Ensures that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

xix. Ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services.

xx. Ensures that the operators of essential services notify, without undue delay, the DSA the incidents having a significant impact on the continuity of the essential services they provide.

xxi. Ensures that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III of Directive (EU) 2016/1148 within the European Union.

xxii. Ensures that the digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III of Directive (EU) 2016/1148 that they offer within the European Union, with a view of ensuring the continuity of those services.

xxiii. Ensures that digital service providers notify the DSA without undue delay, of any incident having a substantial impact on the provision of a service as referred to in Annex III of Directive (EU) 2016/1148, that is offered within the Republic or in any other Member State.

xxiv. Issues decisions within its powers according to the provisions of N.17(I)/18.

xxv. Imposes an administrative fine according to the provisions of article 29 of N.17(I)/18, to any person acts in breach of the provisions of N.17(I)/18 or of any secondary legislation based on the said act.

xxvi. Represent the Republic of Cyprus at any international organisation related to digital security matters.

xxvii. Exercises any other responsibilities, powers and duties which are assigned to the DSA according to N.17(I)/18 or any other secondary legislation based on the said act.

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

There is no specific framework available for seeking compensation for damages resulted due to lack of cybersecurity. However, the general framework provided by the civil code may be used and a case for damages for loss sustained due to negligence or compensation may be claimed based on breach of contractual obligations.

5.4 Enforcement: fines and sanctions

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

For breaches of personal data conducted by processors or controllers or failure to comply with their obligations under N.125(I)/2018, article 33(2) poses a fine of up to 30.000 euro and/or imprisonment of up to 3 years. In cases where such breach constitutes a threat to the interests of the Republic of Cyprus then there would be a fine of up to 50.000 euro and/or imprisonment of up to 5 years.

For breaches related to cyber security, N.17(I)/18 provides at article 16 that in case of a failure to comply with its provisions or of the provisions of secondary legislation based on N.17(I)/18 could lead to a fine of up to 10.000 euro and/or imprisonment of up to 6 months.

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

According to article 32 of the N.125(I)/18, the Commissioner for the Protection of Personal Data may give an administrative fine according to article 83 of the GDPR. Where the person which sustains the fine is a public authority and relates to non-for-profit activity, the fine shall not exceed 200.000 euro.

As it relates to cyber security, according to article 13(κε) of N.17(I)/18, the DSA may give an administrative fine to any person that fails to comply with the provisions of N.17(I)/18 or any secondary legislation based on the said law. Such administrative fine, according to article 30, shall come up to 8.500 euro.

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

All criminal offences established under the relevant legislation shall be prosecuted by Cyprus Police via the office of the Attorney General of the Republic (Law Office of the Republic), after a complaint has been made to the police and an investigation have been conducted in order to support the case before the court.

6 Czech Republic

Radim Polčák (Masaryk University) Petra Lančová (Department of Medical Ethics, Faculty of Medicine, Masaryk University, Brno)

6.1 Informed consent

6.1.1 General Regulatory Framework

Regulation	Link	Type of regulation	Brief description and scope
Usnesení č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky (LZPS)	http://www.psp.cz/en/docs/laws/listina.html (English)	Constitutional law	It contains fundamental human rights and freedoms, including the right to the integrity of the person and his or her privacy and the protection of private and family life.