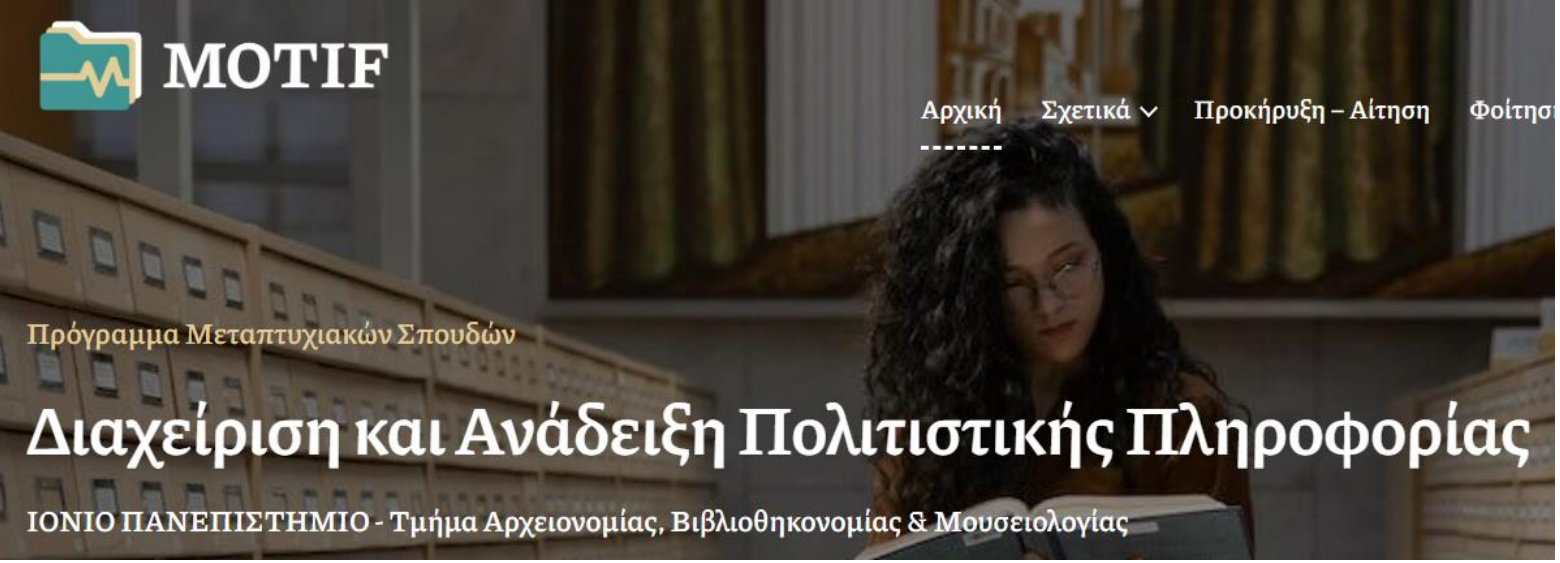
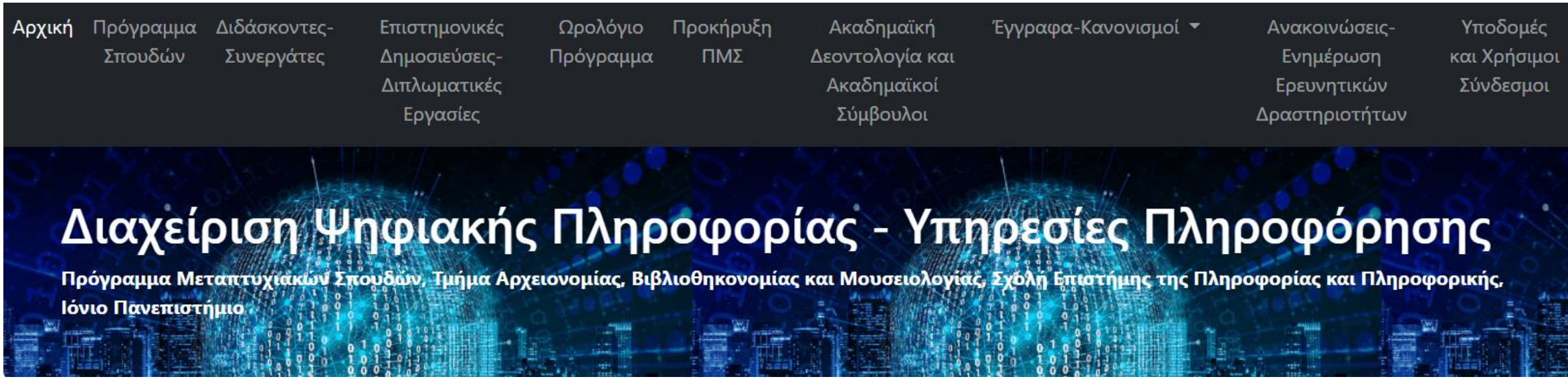


[Διαχείριση και Ανάδειξη Πολιτιστικής Πληροφορίας](): Δίκαιο και Δεοντολογία Πολιτιστικής Πληροφορίας (Υ)



[Διαχείριση Ψηφιακής Πληροφορίας - Υπηρεσίες Πληροφόρησης](): Δίκαιο Πληροφορίας (Ε)

Γιώργος Μπουχάγιαρ
Vrije Universiteit Brussel (Free University of Brussels)
Ιόνιο Πανεπιστήμιο
Email: georgios.bouchagiar@vub.be & georgebouchayar@ionio.gr

CYBER & DATA SECURITY LAB

Ανθρώπινα δικαιώματα

LLN / Προσωπικά δεδομένα *(με παραδείγματα)*

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

- the principle of **lawfulness** requires that the processing be based on a legitimate ground, such as consent. PopEye guarantees there is an appropriate legal basis for any personal data processing operation. Consent is the main legal basis; and volunteer research participants will have the right to withdraw consent to any processing operation. For volunteer research participants, who do not wish to provide consent, identity verification will be performed via the existing, traditional way (passport-check). Moreover, data controllers may choose other legal grounds for the personal data processing (e.g., the contract-basis for the processing of non-biometric data of staff members); albeit, for the processing of special categories of personal data, the exemptions of article 9 of the GDPR (especially 'explicit consent', under GDPR, article 9, para 2, lit a, and the research exception, under GDPR, article 9, para 2, lit j, in conjunction with article 89) should apply.
- the principle of **fairness** demands effective reaction or processing in a rather ethical way and the principle of **transparency** requires full disclosure of relevant information before, during and after the processing operation.[11] PopEye guarantees that all volunteer research participants are given meaningful information in a comprehensive language on all aspects of the Project, including its scope, goals of processing or other procedures (e.g., specific information on how to effectively raise concerns/claims). Furthermore, PopEye ensures that no volunteer research participant is exposed to or bear the consequences of a risk that is greater than that which was initially presented (e.g., by the pilot leaders or technical experts).
- the principle of **purpose limitation** demands that data be '*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*'.[12] PopEye will take all technical and organisational measures to limit the purposes pursued (in case of initial collection) or provide for effective safeguards (in relation to further processing), such as implementation of good encryption schemes to achieve PopEye's research objectives stated in the Project's Grant Agreement (GA).
- the principle of **data minimisation** demands that data be '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'.[13] PopEye will periodically review data held and delete any data that are not strictly necessary to the goals pursued. Notably, PopEye will distinguish between personal data required for administrative purposes and personal data necessary to address research questions.
- under the **accuracy** principle data must be accurate and, where necessary, kept up to date ('*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*').[14] PopEye will take necessary

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

- the principle of **lawfulness** requires that the processing be based on a legitimate ground, such as consent. PopEye guarantees there is an appropriate legal basis for any personal data processing operation. Consent is the main legal basis; and volunteer research participants will have the right to withdraw consent to any processing operation. For volunteer research participants, who do not wish to provide consent, identity verification will be performed via the existing, traditional way (passport-check). Moreover, data controllers may choose other legal grounds for the personal data processing (e.g., the contract-basis for the processing of non-biometric data of staff members); albeit, for the processing of special categories of personal data, the exemptions of article 9 of the GDPR (especially 'explicit consent', under GDPR, article 9, para 2, lit a, and the research exception, under GDPR, article 9, para 2, lit j, in conjunction with article 89) should apply.
- the principle of **fairness** demands effective reaction or processing in a rather ethical way and the principle of **transparency** requires full disclosure of relevant information before, during and after the processing operation.[11] PopEye guarantees that all volunteer research participants are given meaningful information in a comprehensive language on all aspects of the Project, including its scope, goals of processing or other procedures (e.g., specific information on how to effectively raise concerns/claims). Furthermore, PopEye ensures that no volunteer research participant is exposed to or bear the consequences of a risk that is greater than that which was initially presented (e.g., by the pilot leaders or technical experts).
- the principle of **purpose limitation** demands that data be '*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*'.[12] PopEye will take all technical and organisational measures to limit the purposes pursued (in case of initial collection) or provide for effective safeguards (in relation to further processing), such as implementation of good encryption schemes to achieve PopEye's research objectives stated in the Project's Grant Agreement (GA).
- the principle of **data minimisation** demands that data be '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'.[13] PopEye will periodically review data held and delete any data that are not strictly necessary to the goals pursued. Notably, PopEye will distinguish between personal data required for administrative purposes and personal data necessary to address research questions.
- under the **accuracy** principle data must be accurate and, where necessary, kept up to date ('*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*').[14] PopEye will take necessary

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

actions to ensure accuracy of data held; in case of inaccurate/incomplete personal information, PopEye will guarantee that volunteer research participants are offered the opportunity to rectify their data or have them complete.

- the **storage limitation** (or the 'delete') principle requires that data be kept in a form which permits identification *'for no longer than is necessary for the purposes for which the personal data are processed'* (*'personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures'*).[15] PopEye will determine concrete retention periods, in particular relation to the duration of each phase (development, deployment or post-deployment). Even where the above research exemption applies, PopEye will implement all appropriate technical and organisational measures to safeguard the rights and freedoms of volunteer research participants; and, in any event, no data will be kept for longer than actually needed.
- the principle of **data security** (or 'integrity and confidentiality') refers to the processing in a way that guarantees appropriate security (e.g., protection against unauthorised or unlawful processing), using necessary technical/organisational measures.[16] PopEye will implement such measures to enhance security.

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

Moreover, the GDPR and the LED demand that data controllers must fulfil their obligations (e.g., the duty to inform the data subject,[17] explain the rationale behind complex processing operations[18] or abstain from specific automated processing tasks that can have a significant impact on the data subject);[19] and that data subjects enjoy specific rights (e.g., the right to be informed or ask for deletion of data).[20] In this regard, PopEye partners need pay special attention to the following rights:

- **The right to be informed** (GDPR, articles 13 and 14) on any type of personal data processing operation (e.g., collection or further use of personal data). PopEye will inform volunteer research participants on all aspects of the data processing operations that may occur, including the way in which personal data may be used.
- **The right to access personal data and supplementary/additional information** (GDPR, article 15). This must include: the provision of copies of information stored in an appropriate (structured, commonly used and machine-readable) format; and the transferring of personal data to another data controller (where permitted by law). PopEye must timely respond to volunteer research participants' requests. Access requests can be sent via emailing the Project's Data Protection Officer (DPO) or contacting the Project's website.
- **The right to have rectified inaccurate personal data or completed if they are incomplete** (GDPR, article 16). Where the volunteer research participant believes that her/his personal information, undergoing processing, is incorrect or incomplete, she/he will have the right to communicate PopEye by contacting the Project's website and have her/his information rectified or completed.
- **The right to erasure** (GDPR, article 17). At any point in time, volunteer research participants will have the right to request, through the Project's platform or website, the deletion of their data; and these data must be deleted without unreasonable delay.

---

[15] GDPR, art 5 para 1 lit e.
[16] GDPR, art 5 para 1 lit f.
[17] GDPR, arts 12-14; LED, arts 13-15. During the PopEye project, the GDPR primarily applies to the anticipated research activities.
[18] GDPR, arts 13, para 2, lit f; 14, para 2, lit g.
[19] GDPR, art 22; LED, art 11.
[20] GDPR, arts 12ff; LED, arts 12ff.

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

- **The right to restrict processing** (GDPR, article 18). At any point in time, volunteer research participants will be given the opportunity to restrict the processing of their data (e.g., stop data collection or further processing). Volunteer research participants will be enabled to send their restriction-request through the Project's platform or website.
- **The right to data portability** (GDPR, article 20). Volunteer research participants will be granted the opportunity to receive their data in an appropriate (structured, commonly used and machine-readable) format, as well as to transfer these data to another entity. This includes the opportunity to obtain and reuse such data for purposes defined by the volunteer research participant across various services.
- **The right to object to the processing** (GDPR, article 21). Given that consent serves as the primary lawful basis for the processing of personal data, volunteer research participants will be offered the chance to object to that processing, as well as to withdraw consent at any point in time.
- **The rights related to automated decision-making and profiling** (GDPR, article 22). Volunteer research participants will enjoy the right to object to such automated decision-making and profiling and be enabled to effectively exercise this right (e.g., by communicating through the Project's platform or website).
- **The right to withdraw consent at any time** (GDPR, article 7, para 3). Volunteer research participants will be given the chance to withdraw consent and have their information erased at any point in time (e.g., by making a request through the Project's platform or website).
- **The right to complain to the relevant Supervisory Authority (SA)** (GDPR, article 77). In all cases, volunteer research participants will have the right to submit a complaint before the competent Data Protection Authority (DPA). It is added that relevant (contact) information of competent SAs will be provided on the Project's website.

The Project's privacy policy will include all of the above enlisted elements (rights of the data subjects), as well as additional information on concrete personal data processing operations (e.g., collection or management). This privacy policy will make specific reference to the processing of sensitive data (special categories of personal data). It will, moreover, be drafted in a comprehensive manner (e.g., plain language), ensuring that all stakeholders can easily understand and familiarise themselves with its content.

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

3 Impact assessment on privacy, ethical, social and legal issues: DPIA+, FRIA, ALTAI, Ethical AI risk assessment 49

3.1 Interim DPIA+: Background, rationale and required elements (under the Project's DoA and related data protection laws) 49

3.2 Interim FRIA: Background, rationale and required elements (under the Project's DoA and AI-related laws) 50

3.3 PopEye's interim DPIA+ and FRIA 51

3.3.1 Preliminary remarks 51

3.3.2 Data processing operations and their purposes 51

3.3.3 Interference with fundamental rights and freedoms 52

3.3.4 Legality, legitimacy and necessity of technological implementations within (and beyond) the PopEye framework 53

3.3.5 Principles-based approach to PopEye technological implementations 60

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

3 Impact assessment on privacy, ethical, social and legal issues: DPIA+, FRIA, ALTAI, Ethical AI risk assessment 49

3.1 Interim DPIA+: Background, rationale and required elements (under the Project's DoA and related data protection laws) 49

3.2 Interim FRIA: Background, rationale and required elements (under the Project's DoA and AI-related laws) 50

3.3 PopEye's interim DPIA+ and FRIA 51

3.3.1 Preliminary remarks 51

3.3.2 Data processing operations and their purposes 51

3.3.3 Interference with fundamental rights and freedoms 52

3.3.4 Legality, legitimacy and necessity of technological implementations within (and beyond) the PopEye framework 53

3.3.5 Principles-based approach to PopEye technological implementations 60

LLN / προσωπικά δεδομένα

SOS

DPIA

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

LLN / προσωπικά δεδομένα

SOS

DPIA

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

LLN / προσωπικά δεδομένα

SOS

DPIA

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

LLN / προσωπικά δεδομένα

SOS

DPIA

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

LLN / προσωπικά δεδομένα

SOS

DPIA

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

LLN / προσωπικά δεδομένα

SOS

DPIA

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

LLN / προσωπικά δεδομένα

SOS

DPIA

Άρθρο 35

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

LLN / προσωπικά δεδομένα

SOS

DPIA

Άρθρο 35

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

LLN / προσωπικά δεδομένα

SOS

DPIA

Άρθρο 35

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

LLN / προσωπικά δεδομένα

SOS

DPIA

Άρθρο 35

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

LLN / προσωπικά δεδομένα

SOS

DPIA

Άρθρο 35

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

LLN / προσωπικά δεδομένα

SOS

DPIA

7. Η εκτίμηση περιέχει τουλάχιστον:

α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

8. Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

9. Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

10. Όταν η επεξεργασία δυνάμει του άρθρου 6 παράγραφος 1 στοιχείο γ) ή ε) έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης, οι παράγραφοι 1 έως 7 δεν εφαρμόζονται, εκτός εάν τα κράτη μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω εκτίμησης πριν από τις δραστηριότητες επεξεργασίας.

11. Όπου απαιτείται, ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας.

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

3 Impact assessment on privacy, ethical, social and legal issues: DPIA+, FRIA, ALTAI, Ethical AI risk assessment 49

3.1 Interim DPIA+: Background, rationale and required elements (under the Project's DoA and related data protection laws) 49

3.2 Interim FRIA: Background, rationale and required elements (under the Project's DoA and AI-related laws) 50

3.3 PopEye's interim DPIA+ and FRIA 51

3.3.1 Preliminary remarks 51

3.3.2 Data processing operations and their purposes 51

3.3.3 Interference with fundamental rights and freedoms 52

3.3.4 Legality, legitimacy and necessity of technological implementations within (and beyond) the PopEye framework 53

3.3.5 Principles-based approach to PopEye technological implementations 60

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

FRIA

Άρθρο 27

Εκτίμηση επιπτώσεων των συστημάτων ΤΝ υψηλού κινδύνου στα θεμελιώδη δικαιώματα

1. Πριν από την ανάπτυξη συστήματος ΤΝ υψηλού κινδύνου που αναφέρεται στο άρθρο 6 παράγραφος 2, με την εξαίρεση συστημάτων ΤΝ υψηλού κινδύνου που προορίζονται για χρήση στον τομέα που αναφέρεται στο παράρτημα ΙΙΙ σημείο 2, οι φορείς εφαρμογής που είναι οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες και οι φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου που αναφέρονται στο παράρτημα ΙΙΙ σημείο 5 στοιχεία β) και γ) διενεργούν εκτίμηση των επιπτώσεων που μπορεί να έχει στα θεμελιώδη δικαιώματα η χρήση του συστήματος. Για τον σκοπό αυτόν, οι φορείς εφαρμογής διενεργούν εκτίμηση που περιλαμβάνει:

α) περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες το σύστημα ΤΝ υψηλού κινδύνου θα χρησιμοποιείται σύμφωνα με τον επιδιωκόμενο σκοπό του·

β) περιγραφή του χρονικού διαστήματος εντός του οποίου και της συχνότητας με την οποία προορίζεται να χρησιμοποιηθεί κάθε σύστημα ΤΝ υψηλού κινδύνου·

γ) τις κατηγορίες φυσικών προσώπων και ομάδων που είναι πιθανό να επηρεαστούν από τη χρήση του στο συγκεκριμένο πλαίσιο·

δ) τους συγκεκριμένους κινδύνους βλάβης που είναι πιθανό να επηρεάσουν τις κατηγορίες φυσικών προσώπων ή ομάδων προσώπων που προσδιορίζονται δυνάμει του στοιχείου γ) της παρούσας παραγράφου, λαμβανομένων υπόψη των πληροφοριών που δίνει ο πάροχος δυνάμει του άρθρου 13·

ε) περιγραφή της εφαρμογής των μέτρων ανθρώπινης εποπτείας, σύμφωνα με τις οδηγίες χρήσης·

στ) τα μέτρα που πρέπει να λαμβάνονται σε περίπτωση επέλευσης των εν λόγω κινδύνων, συμπεριλαμβανομένων των ρυθμίσεων για την εσωτερική διακυβέρνηση και τους μηχανισμούς υποβολής καταγγελιών.

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

FRIA

Άρθρο 27

Εκτίμηση επιπτώσεων των συστημάτων ΤΝ υψηλού κινδύνου στα θεμελιώδη δικαιώματα

1. Πριν από την ανάπτυξη συστήματος ΤΝ υψηλού κινδύνου που αναφέρεται στο άρθρο 6 παράγραφος 2, με την εξαίρεση συστημάτων ΤΝ υψηλού κινδύνου που προορίζονται για χρήση στον τομέα που αναφέρεται στο παράρτημα ΙΙΙ σημείο 2, οι φορείς εφαρμογής που είναι οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες και οι φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου που αναφέρονται στο παράρτημα ΙΙΙ σημείο 5 στοιχεία β) και γ) διενεργούν εκτίμηση των επιπτώσεων που μπορεί να έχει στα θεμελιώδη δικαιώματα η χρήση του συστήματος. Για τον σκοπό αυτόν, οι φορείς εφαρμογής διενεργούν εκτίμηση που περιλαμβάνει:

α) περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες το σύστημα ΤΝ υψηλού κινδύνου θα χρησιμοποιείται σύμφωνα με τον επιδιωκόμενο σκοπό του·

β) περιγραφή του χρονικού διαστήματος εντός του οποίου και της συχνότητας με την οποία προορίζεται να χρησιμοποιηθεί κάθε σύστημα ΤΝ υψηλού κινδύνου·

γ) τις κατηγορίες φυσικών προσώπων και ομάδων που είναι πιθανό να επηρεαστούν από τη χρήση του στο συγκεκριμένο πλαίσιο·

δ) τους συγκεκριμένους κινδύνους βλάβης που είναι πιθανό να επηρεάσουν τις κατηγορίες φυσικών προσώπων ή ομάδων προσώπων που προσδιορίζονται δυνάμει του στοιχείου γ) της παρούσας παραγράφου, λαμβανομένων υπόψη των πληροφοριών που δίνει ο πάροχος δυνάμει του άρθρου 13·

ε) περιγραφή της εφαρμογής των μέτρων ανθρώπινης εποπτείας, σύμφωνα με τις οδηγίες χρήσης·

στ) τα μέτρα που πρέπει να λαμβάνονται σε περίπτωση επέλευσης των εν λόγω κινδύνων, συμπεριλαμβανομένων των ρυθμίσεων για την εσωτερική διακυβέρνηση και τους μηχανισμούς υποβολής καταγγελιών.

LLN / προσωπικά δεδομένα

Π.χ.: σύνορα

SOS

FRIA

Άρθρο 27

Εκτίμηση επιπτώσεων των συστημάτων ΤΝ υψηλού κινδύνου στα θεμελιώδη δικαιώματα

1. Πριν από την ανάπτυξη συστήματος ΤΝ υψηλού κινδύνου που αναφέρεται στο άρθρο 6 παράγραφος 2, με την εξαίρεση συστημάτων ΤΝ υψηλού κινδύνου που προορίζονται για χρήση στον τομέα που αναφέρεται στο παράρτημα ΙΙΙ σημείο 2, οι φορείς εφαρμογής που είναι οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες και οι φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου που αναφέρονται στο παράρτημα ΙΙΙ σημείο 5 στοιχεία β) και γ) διενεργούν εκτίμηση των επιπτώσεων που μπορεί να έχει στα θεμελιώδη δικαιώματα η χρήση του συστήματος. Για τον σκοπό αυτόν, οι φορείς εφαρμογής διενεργούν εκτίμηση που περιλαμβάνει:

α) περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες το σύστημα ΤΝ υψηλού κινδύνου θα χρησιμοποιείται σύμφωνα με τον επιδιωκόμενο σκοπό του·

β) περιγραφή του χρονικού διαστήματος εντός του οποίου και της συχνότητας με την οποία προορίζεται να χρησιμοποιηθεί κάθε σύστημα ΤΝ υψηλού κινδύνου·

γ) τις κατηγορίες φυσικών προσώπων και ομάδων που είναι πιθανό να επηρεαστούν από τη χρήση του στο συγκεκριμένο πλαίσιο·

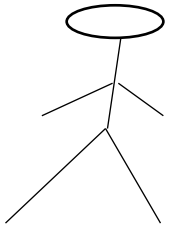
δ) τους συγκεκριμένους κινδύνους βλάβης που είναι πιθανό να επηρεάσουν τις κατηγορίες φυσικών προσώπων ή ομάδων προσώπων που προσδιορίζονται δυνάμει του στοιχείου γ) της παρούσας παραγράφου, λαμβανομένων υπόψη των πληροφοριών που δίνει ο πάροχος δυνάμει του άρθρου 13·

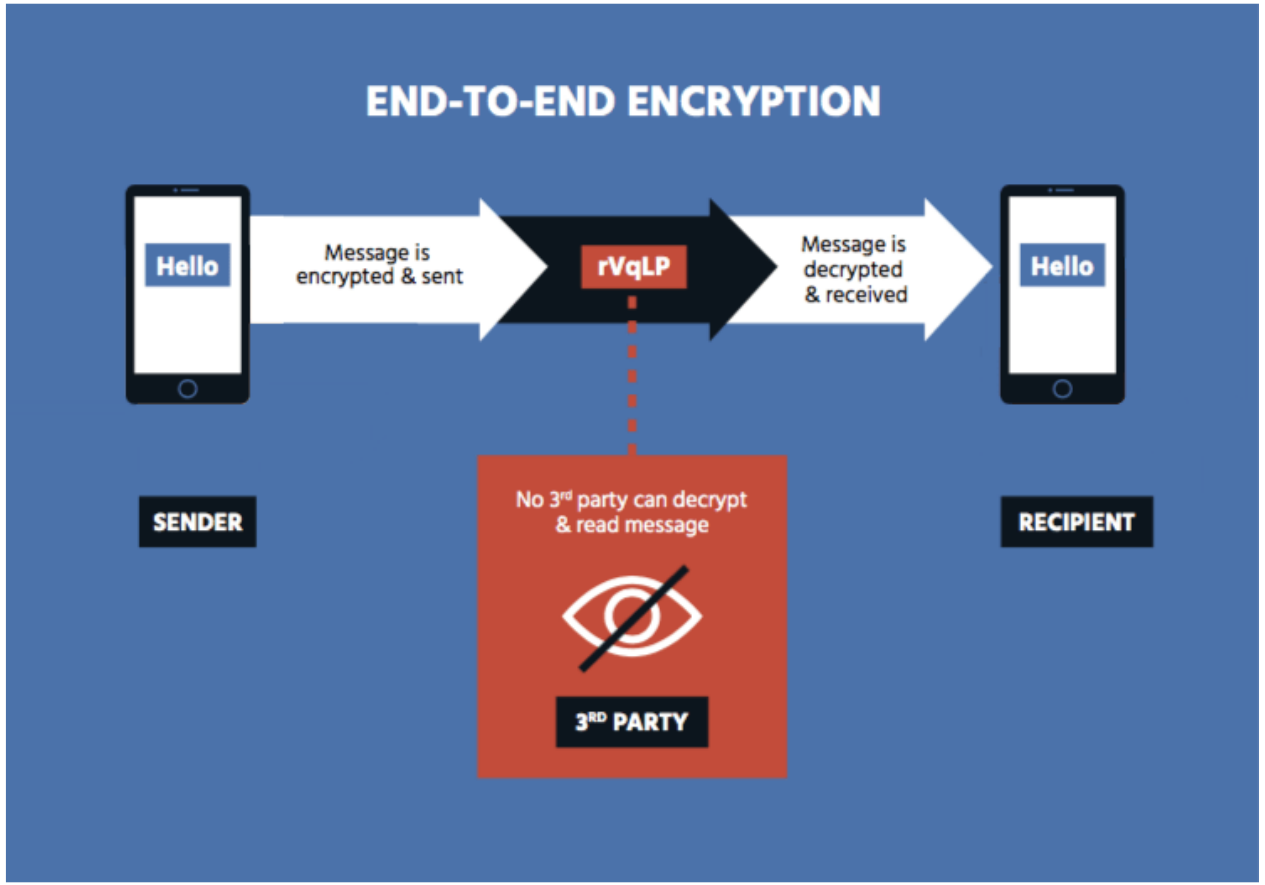
ε) περιγραφή της εφαρμογής των μέτρων ανθρώπινης εποπτείας, σύμφωνα με τις οδηγίες χρήσης·

στ) τα μέτρα που πρέπει να λαμβάνονται σε περίπτωση επέλευσης των εν λόγω κινδύνων, συμπεριλαμβανομένων των ρυθμίσεων για την εσωτερική διακυβέρνηση και τους μηχανισμούς υποβολής καταγγελιών.

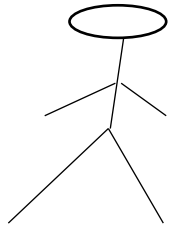
LLN / προσωπικά δεδομένα

Π.χ.: αστυνομία / αποκρυπτογράφηση





Source: Internet Society, '[Encryption Brief]'



Source: https://www.freepik.com/free-photos-vectors/cartoon-police-design#uuid=b96068be-071d-4c81-8a25-e7c4437332b0

SOS

LLN (π.χ.):

- **Ένταλμα** **Legality**
- **Καταπολέμηση εγκλήματος** **Legitimacy**
- **Διασφαλίσεις (όλο το chat?) / άλλα μέσα?** **Necessity**

Ευχαριστώ!!!

Γιώργος Μπουχάγιαρ
Vrije Universiteit Brussel & Ιόνιο Πανεπιστήμιο

Email:
georgios.bouchagiar@vub.be
georgebouchayar@ionio.gr