



EU GDPR - Controller and Processor

Policies and Procedures



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

01	Purpose
02	Scope
03	Sanctions/Compliance
04	EU GDPR Article 2 - Material Scope
05	EU GDPR Article 3 - Territorial Scope
06	EU GDPR Article 4 - Definitions
07	EU GDPR Article 5 - Principles relating to processing of personal data
08	EU GDPR Article 5(1)(f) - Principles relating to processing of personal data - appropriate technical or organisational measures
09	EU GDPR Article 6 - Lawfulness of processing
10	EU GDPR Article 6(4)(e) - Lawfulness of processing - encryption
11	EU GDPR Article 7 - Conditions for consent
12	EU GDPR Article 8 - Conditions applicable to child's consent in relation to information society services
13	EU GDPR Article 9 - Processing of special categories of personal data
14	EU GDPR Article 10 - Processing of personal data relating to criminal convictions and offences
15	EU GDPR Article 11 - Principles relating to processing of personal data
16	EU GDPR Article 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject
17	EU GDPR Article 13 - Information to be provided where personal data are collected from the data subject
18	EU GDPR Article 14 - Information to be provided where personal data have not been obtained from the data subject
19	EU GDPR Article 15 - Right of access by the data subject
20	EU GDPR Article 16 - Right to rectification
21	EU GDPR Article 17 - Right to erasure ('right to be forgotten')
22	EU GDPR Article 18 - Right to restriction of processing
23	EU GDPR Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing
24	EU GDPR Article 20 - Right to data portability
25	EU GDPR Article 21 - Right to object
26	EU GDPR Article 24 - Responsibility of the controller
27	EU GDPR Article 24(1) - Responsibility of the controller - risk assessment

28	EU GDPR Article 24(2) - Responsibility of the controller - policies
29	EU GDPR Article 24(3) - Responsibility of the controller - code of conduct/certification
30	EU GDPR Article 25 - Appropriate technical and organisational measures
31	EU GDPR Article 25(1) - Appropriate technical and organisational measures - data protection
32	EU GDPR Article 25(3) - Appropriate technical and organisational measures - certification
33	EU GDPR Article 26 - Joint Controllers
34	EU GDPR Article 27 - Representatives of controllers or processors not established in the Union
35	EU GDPR Article 28 - Processor
36	EU GDPR Article 28(3) - Processor - contract
37	EU GDPR Article 29 - Processing under the authority of the controller or processor
38	EU GDPR Article 30 - Records of processing activities
39	EU GDPR Article 31 - Cooperation with the supervisory authority
40	EU GDPR Article 32 - Security of Processing
41	EU GDPR Article 32(1)(a) - Security of processing - pseudonymisation and encryption
42	EU GDPR Article 32(1)(b) - Security of processing - confidentiality, integrity, availability and resilience
43	EU GDPR Article 32(1)(c) - Security of processing - restore the availability and access
44	EU GDPR Article 32(1)(d) - Security of processing - effectiveness of measures
45	EU GDPR Article 32(2) - Security of processing - risk assessment
46	EU GDPR Article 32(3) - Security of processing - code of conduct or certification
47	EU GDPR Article 32(4) - Security of processing - processor restrictions
48	EU GDPR Article 33 - Notification of a personal data breach to the supervisory authority
49	EU GDPR Article 33(1) - Notification of a personal data breach to the supervisory authority - by controller
50	EU GDPR Article 34 - Communication of a personal data breach to the data subject
51	EU GDPR Article 34(1-4) - Communication of a personal data breach to the data subject - by controller
52	EU GDPR Article 35 - Data protection impact assessment
53	EU GDPR Article 35(1) - Data protection impact assessment - by controller

54	EU GDPR Article 36 - Prior consultation
55	EU GDPR Article 37 - Designation of the data protection officer
56	EU GDPR Article 37(1) - Designation of the data protection officer - appointment
57	EU GDPR Article 38 - Position of the data protection officer
58	EU GDPR Article 38(1) - Position of the data protection officer - involvement
59	EU GDPR Article 38(2) - Position of the data protection officer - adequate resources
60	EU GDPR Article 38(3) - Position of the data protection officer - independence/direct report
61	EU GDPR Article 38(4) - Position of the data protection officer - data subjects
62	EU GDPR Article 39 - Tasks of the data protection officer
63	EU GDPR Article 39(1)(a) - Tasks of the data protection officer - processor and workforce
64	EU GDPR Article 39(1)(b) - Tasks of the data protection officer - compliance monitoring
65	EU GDPR Article 39(1)(c) - Tasks of the data protection officer - data impact assessment
66	EU GDPR Article 39(1)(d) - Tasks of the data protection officer - supervisory authority cooperation
67	EU GDPR Article 39(1)(e) - Tasks of the data protection officer - contact point
68	EU GDPR Article 39(2) - Tasks of the data protection officer - risk management
69	EU GDPR Article 40 - Codes of conduct
70	EU GDPR Article 40(2)(h) - Codes of conduct - data security
71	EU GDPR Article 40(2)(i) - Codes of conduct - data breach notification
72	EU GDPR Article 41 - Monitoring of approved codes of conduct
73	EU GDPR Article 42 - Certification
74	EU GDPR Article 43 - Certification bodies
75	EU GDPR Article 44 - General principle for transfers
76	EU GDPR Article 45 - Transfers on the basis of an adequacy decision
77	EU GDPR Article 46 - Transfers subject to appropriate safeguards
78	EU GDPR Article 77 - Right to lodge a complaint with the Commissioner
79	EU GDPR Article 79 - Right to an effective judicial remedy against a controller or processor
80	EU GDPR Article 80 - Representation of data subjects
81	EU GDPR Article 82 - Right to compensation and liability

82	EU GDPR Article 83 - General conditions for imposing administrative fines
83	EU GDPR Article 84 - Penalties

Purpose

GDPR applies to any organisation operating within the EU, as well as any organisations outside of the EU which offer goods or services to customers or businesses in the EU.

Scope

This policy applies to the workforce members of organisations that control or process personal data of EU citizens and residents.



Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

EU GDPR Article 2 - Material Scope

EU GDPR - Controller and Processor	Other Requirements
Article 2	N/A
Material Scope	

Policy

The organization will implement internal controls to satisfy the following requirement:

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
 - a. in the course of an activity which falls outside the scope of Union law;
 - b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
 - c. by a natural person in the course of a purely personal or household activity;
 - d. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Guidance

To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- GDPR-1 - Subject Matter, Material Scope, Territorial Scope, Definitions: The protection of natural persons in relation to the processing of personal data is and fundamental right. This Regulation applies to the processing of personal data of data subjects in the European Union/UK wholly or partly by automated means and to the processing other than by automated means of personal data which form part of and filing system or are intended to form part of and filing system. This Regulation applies to the processing of personal data in the context of the activities of and establishment of and controller or and processor in the



European Union/UK, regardless of whether the processing takes place in the European Union/UK or not.

References

- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

EU GDPR Article 3 - Territorial Scope

EU GDPR - Controller and Processor	Other Requirements
Article 3	N/A
Territorial Scope	

Policy

The organization will implement internal controls to satisfy the following requirement:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - b. the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Guidance

In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- GDPR-1 - Subject Matter, Material Scope, Territorial Scope, Definitions: The protection of natural persons in relation to the processing of personal data is and fundamental right. This Regulation applies to the processing of personal data of data subjects in the European Union/UK wholly or partly by automated means and to the processing other than by automated means of personal data which form part of and filing system or are intended to form part of and filing system. This Regulation applies to the processing of personal data in the context of the activities of and establishment of and controller or and processor in the European Union/UK, regardless of whether the processing takes place in the European Union/UK or not.

References

- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

EU GDPR Article 4 - Definitions

EU GDPR - Controller and Processor	Other Requirements
Article 4	N/A
Definitions	

Policy

The organization will implement internal controls to satisfy the following requirement:

For the purposes of this Regulation:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
6. 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities

shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. 'main establishment' means:

a. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

b. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. 'group of undertakings' means a controlling undertaking and its controlled undertakings;

20. 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;



22. 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

. the controller or processor is established on the territory of the Member State of that supervisory authority;

a. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

b. a complaint has been lodged with that supervisory authority;

23. 'cross-border processing' means either:

a. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

b. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ();

26. 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Guidance

Understand the terms used in GDPR.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- GDPR-1 - Subject Matter, Material Scope, Territorial Scope, Definitions: The protection of natural persons in relation to the processing of personal data is and fundamental right. This Regulation applies to the processing of personal data of data subjects in the European Union/UK wholly or partly by automated means and to the processing other than by automated means of personal data which form part of and filing system or are intended to form part of and filing system. This Regulation applies to the processing of personal data in the context of the activities of and establishment of and controller or and processor in the European Union/UK, regardless of whether the processing takes place in the European Union/UK or not.

References

- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

EU GDPR Article 5 - Principles relating to processing of personal data

EU GDPR - Controller and Processor	Other Requirements
Article 5 Principles relating to processing of personal data	N/A

Policy

The organization will implement internal controls to satisfy the following requirement:

1. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. 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 ('accuracy');

e. kept in a form which permits identification of data subjects 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 required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Guidance

Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily



accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- GDPR-2 - Principles and Lawfulness of Data Processing, Consent: Personal data must be securely processed only as necessary for legitimate lawful purposes, in and transparent manner, for no longer than necessary.

References

- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

EU GDPR Article 5(1)(f) - Principles relating to processing of personal data - appropriate technical or organisational measures

EU GDPR - Controller and Processor	Other Requirements
Article 5(1)(f) Principles relating to processing of personal data - appropriate technical or organisational measures	N/A

Policy

The organization will implement internal controls to satisfy the following requirement:

1. Personal data shall be:

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Guidance

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC4.7 - System Security Plans (SSP)/Written Information Security Plans (WISP)/Information Security Management System (ISMS): Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how



security requirements are implemented, and the relationships with or connections to other systems.

References

- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

EU GDPR Article 6 - Lawfulness of processing

EU GDPR - Controller and Processor	Other Requirements
Article 6	N/A
Lawfulness of processing	

Policy

The organization will implement internal controls to satisfy the following requirement:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with a legal obligation to which the controller is subject;

d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

a. Union law; or

b. Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general



conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. 4The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Guidance

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- GDPR-2 - Principles and Lawfulness of Data Processing, Consent: Personal data must be securely processed only as necessary for legitimate lawful purposes, in and transparent manner, for no longer than necessary.

References

- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

EU GDPR Article 6(4)(e) - Lawfulness of processing - encryption

EU GDPR - Controller and Processor	Other Requirements
Article 6(4)(e) Lawfulness of processing - encryption	N/A

Policy

The organization will implement internal controls to satisfy the following requirement:

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Guidance

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Responsibilities

The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CC7.31 - Wireless Authentication & Encryption: Protect wireless access using authentication and encryption.
- CC7.33 - Encrypt Remote Sessions: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- CC7.35 - Encrypt Mobile Devices: Encrypt data on mobile devices and mobile computing platforms.
- CC8.15 - Protect & Restrict Removable Media: Ensure that removable media is protected and its use restricted according to policy.
- CC8.27 - Encrypt Data: Implement a mechanism to encrypt and decrypt data.
- CC12.2 - Protect Physical Media: Protect (i.e., physically control and securely store) system media, both paper and digital.
- CC12.6 - Encrypt Media During Transport: Implement cryptographic mechanisms to protect the confidentiality of data stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- CC13.3 - Encryption of Data in Transit: Implement cryptographic mechanisms to prevent unauthorized disclosure of data during transmission unless otherwise protected by alternative physical safeguards.

References



- GDPR Official Site - https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- GDPR Guidance - <https://gdpr.eu/>
- GDPR checklist for data controllers - <https://gdpr.eu/checklist/>

Truncated Sample Report