UK GDPR - Controller and Processor

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

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

55	UK GDPR Article 37 - Designation of the data protection officer
56	UK GDPR Article 37(1) - Designation of the data protection officer - appointment
57	UK GDPR Article 38 - Position of the data protection officer
58	UK GDPR Article 39 - Tasks of the data protection officer
59	UK GDPR Article 39(1)(a) - Tasks of the data protection officer - processor and workforce
60	UK GDPR Article 39(1)(b) - Tasks of the data protection officer - compliance monitoring
61	UK GDPR Article 39(1)(c) - Tasks of the data protection officer - data impact assessment
62	UK GDPR Article 39(1)(d) - Tasks of the data protection officer - supervisory authority cooperation
63	UK GDPR Article 39(1)(e) - Tasks of the data protection officer - contact point
64	UK GDPR Article 39(2) - Tasks of the data protection officer - risk management
65	UK GDPR Article 40 - Codes of conduct
66	UK GDPR Article 41 - Monitoring of approved codes of conduct
67	UK GDPR Article 42 - Certification
68	UK GDPR Article 43 - Certification bodies
69	UK GDPR Article 44 - General principle for transfers
70	UK GDPR Article 45 - Transfers on the basis of an adequacy decision
71	UK GDPR Article 46 - Transfers subject to appropriate safeguards
72	UK GDPR Article 77 - Right to lodge a complaint with the Commissioner
73	UK GDPR Article 78 - Right to an effective judicial remedy against the Commissioner
74	UK GDPR Article 79 - Right to an effective judicial remedy against a controller or processor
75	UK GDPR Article 80 - Representation of data subjects
76	UK GDPR Article 82 - Right to compensation and liability
77	UK GDPR Article 83 - General conditions for imposing administrative fines
78	UK GDPR Article 84 - Penalties

Purpose

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

Scope

This policy applies to the workforce members of organisations that control or process personal data of UK 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.

UK GDPR Article 2 - Material Scope

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

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

1. This Regulation applies to the automated or structured processing of personal data, including- (a) processing in the course of an activity which, immediately before IP completion day, fell outside the scope of EU law, and (b) processing in the course of an activity which, immediately before IP completion day, fell within the scope of Chapter 2 of Title 5 of the Treaty on European Union (common foreign and security policy activities).

1A. This Regulation also applies to the manual unstructured processing of personal data held by an FOI public authority.

2. This Regulation does not apply to-

(a) the processing of personal data by an individual in the course of a purely personal or household activity;

(b) the processing of personal data by a competent authority for any of the law enforcement purposes (see Part 3 of the 2018 Act);

(c) the processing of personal data to which Part 4 of the 2018 Act (intelligence services processing) applies.

4. This Regulation shall be without prejudice to the application of the Electronic Commerce (EC Directive) Regulations 2002, in particular the provisions about mere conduits, caching and hosting (see regulations 17 to 19 of those Regulations).

5. In this Article –

(a) 'the automated or structured processing of personal data' means-

(i) the processing of personal data wholly or partly by automated means, and

(ii) the processing otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system;

(b) 'the manual unstructured processing of personal data' means the processing of personal data which is not the automated or structured processing of personal data;

(c) 'FOI public authority' has the same meaning as in Chapter 3 of Part 2 of the 2018 Act (see section 21(5) of that Act);

(d) references to personal data 'held' by an FOI public authority are to be interpreted in accordance with section 21(6) and (7) of the 2018 Act;

(e) ‘competent authority’ and ‘law enforcement purposes’ have the same meaning as in Part 3 of the 2018 Act (see sections 30 and 31 of that Act).

Guidance
In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. 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. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC[1].

[1] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) OJ L 124, 20.5.2003, p. 36 (europa.eu).

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
- UK GDPR Official Site - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- UK GDPR Guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/
- Guide to the UK GDPR - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

UK GDPR Article 3 - Territorial Scope

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

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

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 United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.

This Regulation applies to the [relevant] processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom 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 United Kingdom; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the United Kingdom.

2A. In paragraph 2, “relevant processing of personal data” means processing to which this Regulation applies, other than processing described in Article 2(1)(a) or (b) or (1A).]
This Regulation applies to the processing of personal data by a controller not established in the United Kingdom, but in a place where domestic law applies by virtue of public international law.

Guidance
Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

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
- UK GDPR Official Site - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- UK GDPR Guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/

- Guide to the UK GDPR - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

UK GDPR Article 4 - Definitions

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

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

For the purposes of this Regulation:

(A1) 'the 2018 Act' means the Data Protection Act 2018;

(A2) 'domestic law' means the law of the United Kingdom or of a part of the United Kingdom;

(A3) 'the Commissioner' means the Information Commissioner (see section 114 of the 2018 Act);]

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; (but see section 6 of the 2018 Act);

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. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with domestic 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;

(10A) ‘public authority’ and ‘public body’ are to be interpreted in accordance with section 7 of the 2018 Act and provision made under that section;]

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;

17. ‘representative’ means a natural or legal person established in the United Kingdom 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 in the United Kingdom 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;

(21A) foreign designated authority’ means an authority designated for the purposes of Article 13 of the Data Protection Convention (as defined by section 3 of the 2018 Act) by a party, other than the United Kingdom, which is bound by that Convention;)

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

- UK GDPR Official Site - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- UK GDPR Guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/
- Guide to the UK GDPR - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

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

UK 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:

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'); (1) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(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').
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

- UK GDPR Official Site - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- UK GDPR Guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/
- Guide to the UK GDPR - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

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

UK 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

No References.

UK GDPR Article 6 - Lawfulness of processing

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

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

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. The domestic law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

3. 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 domestic law which constitutes a necessary

and proportionate measure in a democratic society to safeguard national security, defence or any of 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:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(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
- UK GDPR Official Site - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- UK GDPR Guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/
- Guide to the UK GDPR - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

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

UK 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
No References.

UK GDPR Article 7 - Conditions for consent

UK GDPR - Controller and Processor	Other Requirements
Article 7 Conditions for consent	N/A

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

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Guidance
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

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

- UK GDPR Official Site - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- UK GDPR Guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/
- Guide to the UK GDPR - https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Truncated Sample Report