GDPR Implementation Standard

Version 1.0

enquiries@claytonsecurity.com
Web www.claytonsecurity.com
Published in the United Kingdom

Table of Contents

1 Introduction

This document contains an implementation standard for the General Data Protection Regulation (GDPR). It is intended as a guide to implementing GDPR Compliance into an organization.

2 History

Version	Description	Date
V 1.0	First draft for public release	29/07/2017

3 Terminology

The use of certain words in this document convey specific meaning which is described below.

Shall Any requirement including the word “shall” is mandatory and in order to comply with this standard the organization must implement the requirement in its entirety.

Should Any requirement including the word “should” is a recommendation and the organization can choose implement the requirement or not with no loss of compliance. However, if the organization adopts the recommendation it shall be implemented in its entirety.

May Any requirement including the word “may” implies a choice and the organization can choose implement the options or not with no loss of compliance.

4 Requirements

4.1 Identifying data

The organization shall identify Personally Identifiable Information (PII) within the scope of GDPR. In order to do this, the organization should create and implement a (GDPR) Data Policy for privacy and protection of personally identifiable information. This policy should be communicated to all interested parties involved in the processing of Personally Identifiable Information.

The policy should cover the following principles/information:

1. Identifying what is PII as it relates to the organization according to Article 4 (1) of GDPR;
2. Whether the PII falls under the scope of GDPR Article 2 (see paragraph 5) and Article 3;
3. Whether the collection of PII is processed according to the principles in Article 5;
4. The nature of the processing and if it is used for direct marketing (Article 21);
5. Whether the PII is subject to automated processing, including profiling;
6. Whether the organization is a controller or processor of data (see GDPR Article 4 points 7 or 8);
7. Whether there are joint controllers of the PII (Article 26).
8. The identity of the GDPR Representative (if the Organization is outside the Union) and contact details (see GDPR Article 4 point 17 and Article 27);
9. How consent has been given and is recorded (Article 7 and Article 8);
10. Justification for lawful processing (Article 6);
11. Whether the data is a special category (Article 9);
12. A record of processing activities under its responsibility (Article 30);
13. The justification for processing data if it is a special category (Article 9);
14. Whether a Data Protection Officer (DPO) is required (see paragraph 14.1) and the contact details of that DPO;

15. The reporting structure if a single DPO is responsible for several departments or organizations;
16. How the information in paragraph 6.1 will be communicated to the data subject (unless exempt under conditions detailed in 6.2);
17. The rights of a data subject to obtain confirmation as to whether or not personal data concerning him or her are being processed (See 7 for details);
18. Where the rights of data subject are publicised (e.g. website) including the charge for additional copies of the personal data;
19. The rights and safeguards if personal data is transferred a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards (Article 46) relating to the transfer.
20. The rights of the data subject to rectify or erase the data.
21. Details of the proof required to ensure that the rectification has come from the data subject.
22. The nature and extent of restriction of processing for the conditions stated in Article 18 (see 12).
23. The justification for not taking reasonable steps to erase personal data that has been made public based on taking account of available technology and the cost of implementation (Article 17)s.
24. The justification for not informing the data subject of to whom the data may have been disclosed, if it proves impossible or involves disproportionate effort (see Article 19).
25. What commonly used and machine-readable format is used to provide the personal data is provided to the data subject (Article 20).
26. Who in the organization is authorized to access the PII (authorized persons).
27. The organization GDPR data breach policy, based on article 33, identifying the contact details of the supervisory authority.
28. Whether the PII is transferred to a third country and details of safeguards put in place (Article 45, see section 13).

4.2 GDPR data register

The organization should create and maintain a GDPR data register which identifies:

1. The description of the data;
2. How the data is considered to fall under the scope of GDPR or not;
3. Whether the data is used for direct marketing (Article 21);
4. Justification for lawful processing (Article 6);
5. Where it has been stored;
6. How it is protected at rest;
7. How it is protected during processing;
8. How consent has been given;
9. Where the consent is recorded;
10. Whether the data is a special category (Article 9);
11. The source of the personal data;
12. Whether the personal data has been supplied to the data subject and details of when and how;
13. Whether the personal data has been changed since being supplied to the data subject;
14. Whether the personal data has been rectified by the data subject;
15. The conditions that would result in data protection impact assessment according to Article 35 (1 (i.e. processing is likely to result in a high risk to the rights and freedoms of natural persons);
16.

5 Exclusions from GDPR

Article 2 defines the material scope of GDPR and contains certain exclusions. The GDPR does not apply to:

1. PII connected with National Security;
2. the processing of anonymous data, i.e. data that cannot be traced back to the individual;

3. the processing of data relating to deceased persons;
4. the processing of personal data of data subjects who are NOT in the Union
5. the processing of data relating to legal persons (company contact and to one-man businesses are considered personal data);
6. physical files or sets of files which are not structured according to specific criteria.
7. the processing of personal data by Member States when carrying out activities in relation to the common foreign and security policy of the European Union;
8. the processing of personal data by a natural person in the course of a purely personal or household activity, such as correspondence, the holding of addresses as well as social networking and online activities in the context of personal and household activities;
9. the processing of personal data by competent authorities for 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;
10. the processing of personal data by European Union institutions, bodies, offices and agencies, in which case Regulation (EC) No 45/2001 applies.

6 Communicating Data subject's rights

6.1 Communication requirements

The organization should conduct a regular review of the communications with data subjects with a view to ensuring that:

1. the identity of the controller of the data, or the controller's representative, is provided;
2. the contact details of the data protection officer, (if a DPO is required) (see section 14.1);
3. the reason for the processing for which the personal data are intended as well as the legal basis for the processing;
4. the legitimate interests pursued by the controller or by a third party if the lawfulness is based on point (f) of Article 6(1);
5. whether controller intends to transfer personal data to a third country or international organisation and the safeguards and the means by which to obtain a copy of them or the details of a decision by the Commission that provides for a transfer;
6. the recipients or categories of recipients of the personal data, if the data will be transferred;
7. the period for which the personal data will be stored;
8. whether the data is subject to automated decision making and/or profiling and the consequences of that automation; and,
9. the means by which the data subject may request from the controller;
    a. access to their personal data,
    b. correction of their personal data,
    c. erasure of their personal data,
    d. restriction of processing open to the data subject,
    e. the right to data portability,
    f. the right to withdraw consent,
    g. how to complain to a member state supervisory body,
    h. whether the data is required by legislation and the consequences of the data subject not providing it.

If it is identified that the data is intended to be processed other than expected when consent was given then the data subject shall be informed.

This information shall be clear and concise.

If the personal data has not been obtained from the data subject the organization shall provide in addition:

1. the categories of personal data concerned; and,
2. the source of the data and if it came from public sources.

This information shall be provided as soon as practicable but no later than one month from the time of collection or at the time of first contact with the data subject whichever is earlier. If the data is to be disclosed to a third party then the information shall be provided prior to its being shared.

6.2 Communication requirements exemptions

The organization shall not inform the data subject if:

1. the data subject already has the information;
2. if the effort to do this is disproportionate to the reason for collecting the data (this is particularly so when processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes);

In the case of 2 above, the organization shall safeguard the rights and freedoms of the data subjects by technical, procedural and/or organization methods.

6.2.1 Protecting the rights of data subjects w.r.t. Communication exemptions

An example of a technical mechanism is pseudonymisation, where the identifying fields are replaced by artificial identifiers. If this is employed then the organization should document a policy for this and a procedure to achieve it. There are two options:

1. to replace the identifying fields with random record I.D.s and maintaining a correlation record set that is protected by encryption mechanisms and to which access is limited, documented and audited regularly; or,
2. Delete permanently the identifying fields.

The policy should contain no less than the requirements in ISO 27001 A.10.1.

The procedural and organization methods should contain no less than the requirements in ISO 27001 A.6.1.2, A.7, A.8.1, A.8.2, A.9, A.11.2.7, A.11.2.8, A.11.2.9, A.12.1.1, A.12.2, A.12.3, A.12.4, etc..

7 GDPR Access Procedure

The organization should create and maintain a GDPR access procedure to describe how to handle access requests from data subjects (Article 15). The procedure should list the information provided to the data subject, which should be no less than:

1. the purposes of the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
6. the right to lodge a complaint with a supervisory authority;
7. where the personal data are not collected from the data subject, any available information as to their source;
8. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
9. the rights of the data subject shall have the right to be informed of the appropriate;safeguards pursuant to Article 46 relating to the transfer if personal data are transferred to a third country or to an international organisation; and,
10. a copy of the personal data undergoing processing.

The first copy shall be free of charge. A reasonable charge may be levied for any further copies requested by the data subject, based on administrative costs as long as the charge is advertised.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy shall not adversely affect the rights and freedoms of others.

8 GDPR data rectification and erasure procedure

The organization should create and maintain a GDPR rectification and erasure procedure that should detail how the personal data of the data subject is rectified and how the personal data is erased. The procedure should identify the maximum time taken to achieve rectification or erasure of the personal data.

In the event of data being erased, the procedure should detail the process in the event:

1. that the personal data are no necessary in relation to the purposes for which they were collected or otherwise processed;
2. that consent has been withdrawn;
3. that the legitimate grounds for keeping the data or processing it have changed;
4. that the personal data has been unlawfully processed;
5. that erasure is due to for compliance with a legal obligation in Union or Member State law to which the controller is subject; and,
6. that the erasure is due to the misapplication of the rules regarding the collection and processing of data of children under the age of 16 years.

It is possible that the procedure for the events listed is the same and/or the time taken to achieve erasure is the same.

The procedure shall also identify the process to identify the process to deny erasure in the event that the personal data is subject to:

1. exercising the right of freedom of expression and information;
2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
3. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
5. for the establishment, exercise or defence of legal claims.

The procedure should list what proof is accepted that the rectification or request for erasure is from the data subject.

The procedure should identify what process is in place to ensure that personal data that is erased is expunged from backups.

The procedure shall also identify the reasonable steps taken to erase the data if it has been made public.

The procedure shall identify how the data subject is informed that rectification or erasure has occurred and, if the data subject requests it, each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

9 Data processing

9.1 Processing records

The organization should create and maintain a GDPR data processing procedure that details:

1. how data is chosen for processing (record of processing activities under its responsibility);
2. how data is excluded from processing if the data subject objects;
3. whether profiling occurs and the nature of this profiling; and
4. whether the processing is automated.

If the Organization employs more than 249 (see Article 30 for other conditions), the organization shall create and maintain a GDPR data processing register that details:

1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
2. the categories of processing carried out on behalf of each controller (if there are different categories);
3. the purposes of the processing;
4. a description of the categories of data subjects and of the categories of personal data;
5. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
6. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
7. where possible, the envisaged time limits for erasure of the different categories of data;
8. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

9.2 Security of processing

The organisation should create and maintain a GDPR data processing security policy that describes the appropriate technical and organisational measures to ensure a level of security of subject data. The level of data security shall be based on a risk assessment of the following:

1. that the subject data is only available to authorized people for the legitimate purpose for which the data is collected (confidentiality);
2. that the subject data is not changed either accidentally or on purpose in a way that infringes the data subject's fundamental rights and freedoms (integrity);
3. the availability to the subject data is maintained in order to fulfil the legitimate purpose for which the data is collected (availability);
4. that the data subject data is protected and that the data is restored in a timely manner in the event of a physical or technical incident (backup and restore);

The organization shall determine who is authorized in the organisation and for what legitimate purpose (see 4.1(26).

When identifying the appropriate security, or Granular Access Control, to apply to subject data organizations may consider options such as:

- encrypting the subject data and controlling access by the use of unique passwords;
- replacing the identifying fields of the subject data record by a unique alpha-numeric identifier (pseudonymisation) and restricting access, further still, to the correlation table;
- physically isolating the subject data and putting in place physical controls to limit access; and,
- combinations of the above.

10 Data Breaches

The organization should create and maintain a GDPR data breach procedure which identifies:

1. Who in the organization shall notify the supervisory authority;
2. The contact details of the supervisory authority, bearing in mind there could be more than one depending on the member state of the affected data subjects;
3. How the time awareness of the data breach will be recorded;
4. How details of the data breach, its effects and the remedial action taken will be recorded;

5. How notification will be made (a standard form in the language of the member state may be defined);
6. What needs to be notified according to Article 33 (3;
7. The conditions that would constitute high risk and trigger communication of the data breach to affected data subjects under article 34 paying particular note to point 3 (the conditions for not informing the affected data subjects);
8. How notification to the affected data subjects will be made (a standard form in the language of the member state may be defined in clear and plain language);
9. What needs to be notified according to Article 34 (2.

11 Data protection impact assessment

If 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. The supervisory authority is required to identify and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.

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

The organization shall consult the supervisory authority if the impact assessment indicates that there would be a high risk to the subject data and the nature of measures taken to mitigate the risk.

12 Restriction of processing

The organization shall identify the procedure to be adopted if the conditions identified in Article 18 (Right to restriction of processing) apply. The procedure should identify the nature of the restriction.

The procedure shall identify how the data subject is informed that restriction has occurred and, if the data subject requests it, each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

13 Transfers of personal data to third countries or international organisations

Where the commission publishes a decision that a third country, or an international organisation, ensures an adequate level of protection, then a transfer shall not require any specific authorisation. If there is doubt, or no such decision has been published by the commission, then the following requirements shall be met before transferring data to a third country or an international organisation.

The organization shall provide appropriate safeguards such as:

1. ensuring that a legally binding and enforceable instrument between public authorities or bodies exists;
2. binding corporate rules exist in accordance with Article 47 or the GDPR; and
3. Compliance with this standard is demonstrated by the third country organization.

See Article 49 or the GDPR for derogations for specific situations.

14 Organization GDPR personnel

14.1 Data Protection Officer (DPO)

The organization shall appoint a Data Protection Officer if:

1. The organization is a public authority or body (except for courts acting in their judicial capacity);
2. The organization processes data on a large scale;
3. The organization processes data included in the special categories (Article 9) on a large scale or personal data relating to criminal convictions and offences (Article 10).

Some member states may require through legislation the appointment of a Data Protection Officer irrespective of the conditions above. This shall be verified and recorded by the organization.

If there are a group of organizations under the control of a single entity then a single DPO may be appointed for those organizations with a reporting structure as defined in the Data Policy (see paragraph 4.1). The data protection officer may act for such associations and other bodies representing controllers or processors. The organization shall ensure that the Data Protection Officer is easily accessible to all members of the group for which they are responsible.

The organization shall ensure that the Data Protection Officer is qualified to hold that position and has expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

15 References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [© European Union, http://eur-lex.europa.eu/, 1998-2016.]

[2] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

16 Important Notices and Disclaimers Concerning Clayton Security Documents

Clayton Security documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning Clayton Security Documents."

16.1 Notice and Disclaimer of Liability Concerning the use of Clayton Security Documents

Clayton Security Standards documents are developed within the Clayton Security. While Clayton Security takes care during the development process, Clayton Security does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of a Clayton Security Standard is wholly voluntary. Clayton Security disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon any Clayton Security Standard document.

Clayton Security does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained in its standards is free from patent infringement. Clayton Security Standards documents are supplied "AS IS."

The existence of a Clayton Security Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the Clayton Security standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every Clayton Security standard is subjected to review on a regular basis, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any Clayton Security standard.

In publishing and making its standards available, Clayton Security is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is Clayton Security undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any Clayton Security Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given Clayton Security standard.