EUROPEAN COMMISSION



**Once-Only domain**

**Data Processing Agreement (Template)**

|  |  |
| --- | --- |
| Once-Only domain Data Processing Agreement (Template) | Version 4.0  18/08/2023 |
|  |

Document Status:

|  |
| --- |
| Status |
| Version 4.00 obsoletes version 3.00 released in July 2023 |

Summary of Changes:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Created by | Short Description of Changes |
| [*https://ec.europa.eu/digital-building-blocks/wikis/x/9obOK*](https://ec.europa.eu/digital-building-blocks/wikis/x/9obOK) *\** | | | |

Contents

[Introduction 3](#_Toc144219253)

[1. Definitions and interpretation 3](#_Toc144219254)

[2. Personal data of the Controller 4](#_Toc144219255)

[3. Compliance with Applicable Legislation 4](#_Toc144219256)

[4. Confidentiality 5](#_Toc144219257)

[5. Security of Processing and Technical and Organisational Measures 5](#_Toc144219258)

[6. Sub-processing 5](#_Toc144219259)

[7. Data Subject rights 6](#_Toc144219260)

[8. Security Incidents 6](#_Toc144219261)

[9. Data Protection Impact Assessment and Prior Consultation 6](#_Toc144219262)

[10. Erasure or return of the Processor Personal Data 7](#_Toc144219263)

[11. Transfers of Personal Data to third countries 7](#_Toc144219264)

[12. Term and termination 7](#_Toc144219265)

[13. Liability 7](#_Toc144219266)

[14. General 7](#_Toc144219267)

[15. Signature Page 9](#_Toc144219268)

[ANNEX I 10](#_Toc144219269)

# 

This template for a Data Processing Agreement (the Agreement on Data Processing) sets out technical requirements for the Controller and the to follow when processing Personal Data. This template should be used by the Competent Authorities when, at a national level, third parties are instructed by the Competent Authorities to process Personal Data for the Exchange of Evidence through the OOTS.

This DATA PROCESSING AGREEMENT has been concluded on [date].

BETWEEN

* + 1. **[PLACEHOLDER DETAILS COMPETENT AUTHORITY (IN CAPACITY AS EVIDENCE REQUESTER)]**, hereinafter referred to as the **Controller**; and
    2. **DETAILS PROCESSORS [name]**, a [company type] company under [country] law, having its registered office at [address], hereinafter referred to as the **Processor**.

The Parties mentioned sub (1) and (2) are hereinafter also referred to collectively as the **Parties** and individually as a **Party**.

# Introduction

In its capacity as Competent Authority of a Member State within the Once-Only domain, the Controller enters into the present Agreement on Data Processing with the Processor. The Parties wish to establish their rights and obligations with regard to the Processing (as defined below) of Personal Data (as defined below) by the Processor on behalf of the Controller.

**THE PARTIES HAVE AGREED AS FOLLOWS**

# 1. Definitions and interpretation

* 1. The terms which follow shall have the following definitions, notwithstanding any other meaning given to such terms in the Data Processing Agreement:
* “**Agreement**” means this Data Processing Agreement and its annex(es), as in force and amended from time to time;
* “**Applicable Legislation**” means all laws, acts, regulation and legislation as applicable to each Competent Authority, including but not limited to Union Laws on the protection of personal data, in particular, General Data Protection Regulation (EU) 2016/679 (GDPR), Regulation (EU) 2018/172), the ePrivacy Directive (EU) 2002/58/EC, red jointly with all recommendations, opinions and decisions of the relevant authorities.
* “**Authorised User**” means any natural person acting on behalf of a Competent Authority;
* “**Controller**” means a Competent Authority which, acting as Evidence Requester and / or Evidence Provider, determines the purposes and means of the Processing of Personal Data as defined under Regulation (EU) 2016/679;
* “**Competent Authority**” means any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by Regulation (EU) 2018/1724;
* “**Data Subject**” means any User insofar they are natural persons or Authorised Users;
* “**Evidence**”means any document or data, including text or sound, visual or audio-visual recording, irrespective of the medium used, required by a Competent Authority to prove facts or compliance with procedural requirements referred to in point (b) of Article 2(2) of Regulation (EU) 2018/1724;
* “**Evidence Requester**” means a Competent Authority responsible for one or more of the procedures referred to in Article 14(1) of Regulation (EU) 2018/1724;
* “**Evidence Provider**” means a Competent Authority as referred to in Article 14(2) of Regulation (EU) 2018/1724 that lawfully issues structured or unstructured Evidence;
* “**GDPR**” means 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);
* “**OOTS**”means the technical system for the cross-border automated exchange of Evidence referred to in Article 14(1) of Regulation (EU) 2018/1724;
* “**Personal Data**” means any information relating to an identified or identifiable natural person as defined under Article 4(1) Regulation (EU) 2016/679;
* “**Processing Activities**” means any operation or set of operations which is performed on Personal Data or 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, as defined under Article 4 (2) Regulation (EU) 2016/679;
* “**Processor**” means a natural person and or legal entity that processes Personal Data under the Controller's instructions, as defined under Regulation (EU) 2016/679;
* “**Security Incident**” means any unauthorised or unlawful access, alteration, deletion, mutilation, loss or any form of unauthorised or unlawful Processing of Personal Data, or any other incident which shall lead (or may lead) to the accidental or unlawful deletion, loss, modification, unauthorised disclosure of – or access to – the Personal Data, any Personal Data Breach as defined in the GDPR, or any indication that a breach of that nature shall occur or has occurred;
* “**Services**” means the access to the OOTS by the Competent Authorities to facilitate and to perform the exchange of Evidence, including but not limited to acting as Evidence Requester and / or Evidence Provider by the Competent Authorities;
* **“User”** means a citizen of the Union, a natural person residing in a Member State or a legal person having its registered office in a Member State, and who accesses the information, the procedures, or the assistance or problem-solving services, referred to in Article 2(2) of the Regulation (EU) 2018/1724, through the gateway. To avoid any misunderstanding, this excludes the Authorised Users.

# 2. Personal data of the Controller

* 1. The Controller and the Processor acknowledge that the Processor will process Personal Data or other personal information from the Data Subjects. The performance of the Services will involve the processing, transfer and/or storage of such Personal Data by the Processor as “Processor” to the benefit and on behalf of the Controller in its capacity of “Controller”.
  2. The Processor warrants that Personal Data will only be processed, transferred and/or stored only insofar required for the performance of the Services.
  3. A list of the categories and types of Personal Data as well as the purposes for which Personal Data is processed for the benefit of the Controller, the subject matter and duration of the processing, the nature and means of the processing and the categories of Data Subjects has been included in this Data Processing Agreement.

# 3. Compliance with Applicable Legislation

* 1. The Processor shall comply with all Applicable Legislation when processing Personal Data.
  2. The Processor shall process Personal Data following the Controller’s documented instructions (including with regard to transfers of Personal Data to a third country or an international organisation).
  3. The Processor shall not disclose Personal Data directly or indirectly to any person, another controller or governmental entity. If such disclosure is necessary for the proper processing of Personal Data, this may only occur after prior written permission of the Controller and then only under a full obligation of confidentiality and in accordance with the legal requirements of the GDPR.
  4. Other Processing Activities shall only be performed, (i) when the Processor is explicitly instructed to do so by the Controller or (ii) to comply with a legal requirement, after having notified the Controller. Under no circumstances shall the Processor process Personal Data on its own behalf nor on behalf of third parties unless explicitly instructed by the Controller.
  5. The Processor shall take all necessary steps to ensure that any natural person acting under its authority and/or on its behalf does not process Personal Data in contravention with the Applicable Legislation.
  6. The Processor shall process Personal Data verifiably, properly and carefully and in accordance with all applicable data protection regulations and shall not, by any act or omission, put the Controller in breach of any data protection regulations in connection with this Data Processing Agreement.
  7. The Processor shall comply with all reasonable instructions provided by the Controller in relation to the processing of Personal Data. The Processor shall immediately notify the Controller if, in its view, any instructions are in conflict with national law or Union law (including but not limited to the GDPR).
  8. If the Processor infringes on this Agreement by determining its own purposes and means of processing, the Processor shall be considered to be a “Controller” in respect of said Processing Activities and the Controller shall bear no liability whatsoever and will be held harmless by the Processor in this respect.

# 4. Confidentiality

* 1. The Processor shall inform any person, including but not limited to employees, civil servants, interim staff or self-employed workers, who has access to Personal Data of the obligations resting on the Processor with regard to the Controller’s Personal Data.
  2. The Processor shall make sure that all persons involved in the processing of the Controller’s Personal Data are subject to professional or statutory obligations of confidentiality, with the purpose of safeguarding the confidentiality and integrity of the Controller’s Personal Data.

# 5. Security of Processing and Technical and Organisational Measures

* 1. The Processor shall keep the Controller’s Personal Data (physically and logically) separate from any data belonging to the Processor and/or third parties and ensure that the Controller’s Personal Data is under no circumstances combined or mixed with any other data.
  2. The Processor shall implement and maintain all adequate and appropriate technical and organisational measures and controls to prevent unauthorised or unlawful processing of Personal Data and accidental loss, alteration, destruction, damage, theft, use or (unauthorised) disclosure of such Personal Data, and shall protect against any anticipated threats or hazards to the security or integrity of Personal Data, and detect and prevent unlawful or unauthorised processing of, or unlawful or unauthorised access to Personal Data, and such measures shall at a minimum meet the standard required by the Applicable Legislation (including but not limited to the standard required by Article 32 of the GDPR) ensuring the protection of the Data Subject’s rights.
  3. Such measures shall provide a level of security which could be considered as appropriate considering the technical standards and the kind of Personal Data processed, taking into account the state of the art, and the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
  4. The Parties acknowledge that security requirements are changing continually, and that effective security requires a frequent assessment and regular improvement of security measures. The Processor shall therefore continually assess and tighten, supplement or improve the measures implemented for the continued compliance with its obligations.
  5. The Processor shall provide the Controller with a full and clear description, in a transparent and understandable manner, of the manner in which the Processor processes the Controller’s Personal Data and the manner and means in which Personal Data is secured.
  6. The Processor shall maintain a record of all categories of Processing Activities carried out on behalf of the Controller, containing:

1. the name and contact details of the Controller and the data protection officer;
2. the categories of processing carried out on behalf of the Controller;
3. a general description of the technical and organisational security measures.

# 6. Sub-processing

* 1. The Processor shall not subcontract the Processing Activities to a sub-processor without prior written consent of the Controller. In the event that the Controller provides its consent, the Processor shall (prior to the sub-processor processing Personal Data) enter into an agreement with the sub-processor on terms that provide no less protection for the Personal Data than those set out in this Agreement and shall ensure that the agreement with the sub-processor remains in force for the duration of the sub-processor's processing of Personal Data.
  2. If the Controller has previously consented to any subcontracting of the processing of Personal Data in accordance with the terms of any agreement, the Processor shall ensure that the Processing of Personal Data by the sub-processor is on terms that provide no less protection for Personal Data than those set out in this Data Processing Agreement.
  3. The Processor shall ensure that each sub-processor complies with the provisions of this Agreement. The Processor shall remain fully liable for the acts and omissions of each sub-processor.

# 7. Data Subject rights

* 1. Taking into account the nature of the processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, to respond to requests of Data Subjects exercising their rights under the Applicable Legislation.
  2. Any technical or organisational restrictions that would negatively impact the Data Subjects rights and legal timeframe to answer the Data Subjects should be communicated to the Data Controller without undue delay.
  3. The Processor shall promptly and without undue delay, and at least within 72 hours, notify the Controller in writing of all Data Subject requests, enquiries or complaints it receives (including any request by a Data Subject to exercise their rights under the Applicable Legislation). The Processor shall comply with the Controller’s instructions with respect to the request or notice and shall not reply to this request or notice without instruction from the Controller.
  4. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, and provide its full and timely cooperation to the Controller in order to respond to requests for exercising the Data Subject's rights in accordance with the GDPR, after having obtained the approval from and having been instructed by the Controller.
  5. The Processor shall notify without undue delay the Controller of any inquiry into or a seizure by government authorities of Personal Data, or the presumption of such an occurrence, unless a law prohibits such information on important grounds of public interest.

# 8. Security Incidents

* 1. The Processor shall immediately notify the Controller of each Security Incident of which it becomes aware relating to Personal Data and shall provide such assistance in relation to each Security Incident as is reasonably requested by the Controller.
  2. The Processor shall document any Security Incident, comprising the facts relating to the Security Incident, any useful information on the origin, nature, scope and consequences of the Security Incident, the risk that Personal Data have been or may be unlawfully processed, the type, categories and specific Personal Data unlawfully processed, the remedial action that have been or shall be taken and all relevant information. The Processor shall share this information with the Controller within 12 hours, to allow the Controller to comply with the requirements of the Applicable Legislation regarding (i) informing the competent authorities and the Data Subjects without undue delay taking into account the terms for such notification as set out in the GDPR (72 hours after having become aware of a Security Incident), and (ii) the implementation of all necessary remedies.
  3. The Processor shall without any delay remedy any negative consequences arising from an Incident and/or reduce any further consequences to a minimum.
  4. The Processor shall implement without any delay all remedies requested by the Controller or the competent authorities to fix any Security Incident, security breach or any other non-compliance and/or mitigate the risks associated with it. The Processor shall at all times cooperate with the Controller and observe the Controller’s instructions, so as to enable the Controller and/or any third party mandated by the Controller to perform a proper inquiry into the Security Incident, formulate a correct response and subsequently take adequate action with respect to the Security Incident.
  5. If such is deemed necessary by the Controller, the Controller shall inform directly the Data Subjects and other third parties, including the supervisory authority, about any Security Incidents. It is not permitted for the Processor to provide information about Security Incidents to Data Subjects or other third parties, except if the Processor is obliged by law to do so.

# 9. Data Protection Impact Assessment and Prior Consultation

1. The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of the Processor by Article 35 or 36 of the GDPR or equivalent provisions of any other Applicable Legislation, in each case solely in relation to processing of Personal Data by, and taking into account the nature of the processing and information available to, the Processor.

# 10. Erasure or return of the Processor Personal Data

* 1. The Processor shall, unless the Applicable Legislation requires storage of Personal Data, (i) securely return to the Controller or (ii) securely destroy (at the Controller's option) all Personal Data, together with all copies in any form and in any media, in the Processor's power, possession or control promptly following the earliest of:

1. termination or expiry of the contractual agreement with the Controller;
2. a written request from the Controller; or
3. if the Processor no longer needs the Personal Data in connection with the performance of its obligations under the Agreement between the parties.
   1. At the Controller’s request the Processor shall provide proof of the fact that Personal Data have been deleted or removed. The Processor shall certify its compliance with this clause in writing.
   2. Upon expiry of the Agreement, for whatever reason, the Processor shall notify all third parties involved in the processing of Personal Data of the termination of this Data Processing Agreement. The obligations under this clause apply by analogy to these third parties, which the Processor shall ensure and for which the Processor safeguards and holds harmless the Controller. The Processor shall warrant that all third parties involved shall give effect to these and shall indemnify and hold harmless the Controller in this respect.

# 11. Transfers of Personal Data to third countries

* 1. The Processor shall not transfer any Personal Data outside of the European Economic Area (EEA), unless the Controller has given its prior written consent thereto. Such consent may be made subject to the Processor implementing appropriate safeguards (including but not limited to standard contractual clauses or binding corporate rules according to Articles 45 to 47 of the GDPR).

# 12. Term and termination

* 1. The Controller is entitled to terminate this Data Processing Agreement with immediate effect and without prior judicial intervention if it becomes apparent and/or if the Processor states that it cannot, or no longer, meet the requirements which, on the basis of the developments in legislation and/or case law are imposed on the processing of Personal Data. If the Controller were to terminate this Data Processing Agreement with immediate effect due to a breach of this Agreement, the Processor is not entitled to any compensation for damages arising out of or related to such termination.

# 13. Liability

* 1. The Processor shall indemnify and keep indemnified the Controller and any third party beneficiaries for all principal sums, interest and expenses from and against all actions, claims by third parties as well as any and all expected or unexpected losses, damage (including any loss of customers or prejudice to the image or reputation of the Controller), costs, fines or penalties (including penalties imposed by any supervisory authority), and other liabilities which are incurred or sustained by the Controller or third party beneficiaries and either directly arise from or occur in connection with a breach on the part of the Processor, its representatives, its employees and/or its sub-processors authorised in accordance with clause 6, in the performance of its obligations under this Data Processing Agreement. No limitation of liability shall apply in that case.

# 14. General

* 1. During the term of this Data Processing Agreement, the Controller and/or independent third-part auditor appointed by the Controller will have the right to audit the Processors’ compliance with the Applicable Legislation and the provisions set out in this Data Processing Agreement.
  2. If any provision of this Data Processing Agreement is held to be illegal, invalid or unenforceable in whole or part, that provision shall be deemed not to form part of this Data Processing Agreement and the legality, validity and enforceability of the remainder of this Data Processing Agreement shall remain unaffected.
  3. This Data Processing Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the governing law provisions set out in the contractual agreement with the Processor or, if there are no written agreements, the laws of the country in which the Controller is established.
  4. The Parties hereby agree to submit to the jurisdiction and dispute resolution provisions in respect of all disputes arising out of or in connection with this Agreement or, if there are no written agreement, the Parties agree to submit to the exclusive jurisdiction of the courts of the country in which the Controller is established.

# 15. Signature Page

This Data Processing Agreement has been concluded in two (2) originals, each Party acknowledging receipt of one signed original:

For the Controller

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

Function:

For the Processor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

Function:

# ANNEX I

DETAILS OF PROCESSING OF PERSONAL DATA [PROCESSING ACTIVITY]

* 1. Subject matter and duration of the Processing of Personal Data
  2. The obligations and rights of the Controller
  3. The purpose of the Processing of Personal Data
  4. The nature and context of the Processing of Personal Data
  5. The Types of Personal Data to be processed
  6. The categories of Data Subjects to whom the Personal Data Relates
  7. Technical and Organisational Measures