

Protection of Personal Data

1. Purpose

This document describes how the European Chemicals Agency complies with its obligation to protect personal data processed by the Agency, whatever its form, as foreseen under Regulation (EC) No 45/2001.

2. Scope

The Procedure is applicable to the ECHA Secretariat, including when it deals with members of ECHA bodies and the Board of Appeal. It also applies to processors who process personal data on behalf of the Agency.

Linkage to ECHA Process System

L1. Activity:	12. Management
L2. Process:	12.03. Providing Executive Management
L3. Sub-process:	12.03.08. Protecting personal data

3. Description

Personal data protection is consisting of a set of principles which have to be applied in all activities in the Agency by the controllers designated by the Executive Director, under the supervision of a Data Protection Officer who supports and monitors the implementation of the data protection rules in the Agency.

3.1. Process description

3.1.1. Appointment and tasks of the Data Protection Officer

The Data Protection Officer is appointed by a specific decision of the Executive Director, in compliance with article 24 of Regulation (EC) 45/2001 and paragraph A.1 of decision ED/32/2010. Immediately after the appointment, the Agency shall inform the European Data Protection Supervisor of this decision. The Data Protection Officer shall not be dismissed from his position without the prior consent of the European Data Protection Supervisor.

The tasks of the Data Protection Officer are listed in Article 24 and the annex to Regulation (EC) 45/2001, and in decision ED/32/2010:

- Information, advisory and raising awareness function (see 3.1.9)
- Organisational function (see 3.1.7)

Protection of Personal Data

- Cooperative function (see 3.1.8 and 3.1.10)
- Monitoring of compliance, enforcement and handling of complaints and personal data breaches (see 3.1.11, 3.1.12 and 3.1.13).

The implementation of these tasks is done through an annual work plan of the Data Protection Officer, which is presented to the Executive Director and the Directors of the Agency. This action plan includes in particular the operations planned by the Data Protection Officer for implementing the above mentioned tasks. The plan indicates also the resources devoted to data protection in the Agency. An annual report relating to the achievements during the previous year shall be presented to the Executive Director and the Directors of the Agency during the first quarter of the following year.

The Data Protection Officer is closely following all relevant developments in the field of data protection and attends regular training on the topic. S/he also takes part in the regular meetings of the Data Protection Officer's network, where best practices are shared among colleagues from other EU institutions, bodies and agencies.

3.1.2. Nomination and tasks of the Controllers

The Executive Director has formally nominated as controllers the Heads of Unit at ECHA for the activities and processes managed in their respective unit (Decision ED/32/2010). Other staff members may be designated by decision of the Executive Director for specific data processing.

The tasks of the controllers are listed in decision ED/32/2010 (paragraphs B1 to B4) and derive from Regulation (EC) 45/2001. In particular, they have to ensure that personal data is:

- processed fairly and lawfully
- collected for specified, explicit and legitimate purposes
- adequate, relevant and not excessive in relation to that purpose
- accurate and where necessary kept up-to-date
- kept no longer than is necessary for the purpose (reasonable retention times)
- only transferred in line with the provisions of Articles 7-9 of Regulation (EC) 45/2001.

In addition, the controller has to:

- provide the data subjects with the necessary information about the processing (see 3.1.3)
- enable and actively support the exercise of the rights of the data subjects (see 3.1.4)
- ensure data protection compliance by the processors acting on his or her behalf (see 3.1.5)
- implement the necessary security measures to guarantee the protection of the personal data processed (see 3.1.6)
- notify all processes involving personal data to the Data Protection Officer (see 3.1.7)
- provide all necessary information to and cooperate fully with the Data Protection Officer and the European Data Protection Supervisor (see 3.1.8, 3.1.11, 3.1.12 and 3.1.13).

In order to implement these requirements, the job descriptions of the Heads of Unit include a reference to their role as controller, and their performance in the field is taken into account in their annual appraisal. They are invited regularly to participate in a data protection training or workshop organised by the Data Protection Officer. They have to

plan the training of the staff under their responsibility in the field of personal data protection, and they must monitor the compliance of the processes under their responsibilities.

3.1.3. Information to data subjects

The controllers shall inform the data subject when his or her personal data is processed and shall at least include the following information:

- the identity of the controller;
- the purpose of the processing;
- the recipients of the data;
- the existence of the right of access to, and the right to rectify, the data concerning him or her.

Where possible, this shall be complemented with the following additional information:

- the legal basis of the processing;
- the retention period of the data;
- the right to have recourse to the European Data Protection Supervisor.

In practice this obligation shall be implemented mainly via making available to the data subjects specific data protection notices and/or privacy statements. The Data Protection Officer can advise the controllers on the content of such documents.

3.1.4. Facilitating rights of data subjects

The data subjects have certain rights under Regulation (EC) 45/2001 that can be exercised under certain conditions, such as:

- the right of access to one's personal data;
- the right to rectify inaccurate or incomplete personal data;
- the right to blocking of one's personal data;
- the right of erasure of personal data which is processed unlawfully;
- the right to object to the processing on compelling legitimate grounds.

The controller shall facilitate these rights of the data subjects upon simple request and ensure that they are implemented without undue delay. With regard to the right of access to one's personal data, the access shall be provided at the latest within three months from the receipt of the request.

3.1.5. Personal data processing on behalf of the Agency

In some cases ECHA is collaborating with external service providers, who might process personal data on behalf of the Agency. A processor shall only act on instructions from the controller. These activities are as a rule governed by a service contract holding the conditions under which the data can be processed. The contract holds provisions on security, confidentiality and data protection. The contract manager and the controller shall communicate to the processor their obligations in this regard and follow-up on the level of compliance, possibly via checks and audits. All liability issues are settled in the contract, while any breach of the contractual provisions can lead to damages, termination of the contract or any other consequence stipulated in the contract.

3.1.6. Implementation of appropriate security measures

The controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data protected, in line with Articles 21 and 22 of Regulation (EC) 45/2001.

More in particular s/he shall apply all security policies, information security policies and information management policies in force at the Agency. Practical implementation shall include among others:

- safe storage of physical files containing personal data;
- safe storage of electronic files containing personal data;
- secure management of access rights with regard to files containing personal data;
- where necessary, measures that render the data unintelligible to any person who is not authorised to access it (e.g. via data encryption);
- secure transfer and disposal of files containing personal data;
- accurate application of the security classification system in force at the Agency;
- application of reasonable retention periods;
- ensure that processors apply an equivalent level of security when processing personal data on behalf of the Agency.

3.1.7. Identification and notification of processes involving personal data

The controller shall notify all processes involving personal data to the Data Protection Officer (Article 25 of Regulation (EC) 45/2001).

To assist the controllers in this task, the Data Protection Officer has drafted an inventory containing all processing operations where personal data is processed. This inventory is revised regularly in cooperation with the controllers and is used by the Data Protection Officer to follow-up on the controllers' notification duty. Regular reminders are sent to the controllers if notifications are not made. At the same time the document also serves as a basis for the controllers to identify and coordinate the efforts needed in this field.

To facilitate the notification process, the Data Protection Officer has made available an electronic notification form, which is linked to an electronic register of notifications. All notifications made via the form are thus automatically entered into the register of notifications. However, a quality review of the notifications made is undertaken by the Data Protection Officer through bilateral contacts to ensure the quality of the information provided. To finalise the process, a dated and signed paper version of the notification is requested to be entered in a duplicate, paper-based register.

3.1.8. Prior checking by the European Data Protection Supervisor

Processes which pose specific risks to the rights and freedoms of data subjects, such as those involving processing of information related to health, criminal offences or the evaluation of personal aspects of an individual, shall be subject to prior checking by the European Data Protection Supervisor (Article 27 of Regulation (EC) 45/2001).

For this purpose the Data Protection Officer shall analyse the incoming notifications from the controllers and decide (possibly after consulting the European Data Protection Supervisor) whether prior checking is necessary.

Protection of Personal Data

When the necessity is established, the Data Protection Officer shall collect from the controller all necessary information and documents and shall transfer them to the European Data Protection Supervisor, together with a prior checking notification.

The European Data Protection Supervisor shall deliver his or her opinion within two months following receipt of the notification. When the complexity of the matter so requires, this period may also be extended for a further two months. If the opinion has not been delivered by the end of the two-month period, or any extension thereof, it shall be deemed to be favourable. The European Data Protection Supervisor may also request any additional information as is deemed necessary and the deadlines shall be suspended for that time.

The opinion shall be delivered to the controller, who shall inform the European Data Protection Supervisor within three months of the follow-up that was given to his or her recommendations. The Data Protection Officer shall monitor the implementation of the Supervisor's recommendations by the controller.

Subsequently, the European Data Protection Supervisor shall either close the case or request further action. Where the controller does not modify the processing operation accordingly, the European Data Protection Supervisor may exercise the powers granted to him or her under Article 47(1) of Regulation (EC) 45/2001.

3.1.9. Awareness raising and advice

As the Data Protection Officer is responsible for informing the data subjects of their rights and for informing the controllers and the Agency of their obligations and responsibilities, raising awareness is an important task of the Data Protection Officer. In this context, s/he organises regular training for the ECHA staff, as well as specific data protection workshops for specific target groups, and organises awareness raising events.

The Data Protection Officer shall also serve as the single point of contact within the Agency, both internally and for external partners of the Agency, for any questions and requests for advice on specific issues of data protection.

The advice is thus provided by the Data Protection Officer on request of the Executive Director, of a controller, of the Staff Committee or of any individual, or at his/her own initiative. The advice should be provided within 15 working days from the date of the request. If this deadline proves impossible, the Data Protection Officer informs the requester of the delay and indicates a date for delivery. The advice may be published on ECHA's intranet (in an anonymous version) for the benefit of others if the Data Protection Officer considers it useful.

3.1.10. Cooperation with the European Data Protection Supervisor

The Data Protection Officer shall serve as the first point of contact for the European Data Protection Supervisor within the Agency. S/he shall respond to his or her requests and cooperate with the European Data Protection Supervisor at his or her request of at own initiative.

The Data Protection Officer may consult the European Data Protection Supervisor on any issues related to the protection of personal data and refer to him or her any breach of Regulation (EC) 45/2001, which is beyond his powers.

3.1.11. Handling of queries or complaints

Any data subject can address a complaint to ECHA's Data Protection Officer with regard to the processing of his personal data by the Agency. The complaint shall be processed in line with the procedure foreseen in decision ED/32/2010.

The Data Protection Officer shall acknowledge the receipt within 15 working days, in accordance with Article 14 of the Code of Good Administrative Behaviour for the Staff of the European Chemicals Agency in their relations with the public, and verify whether the request is to be treated as confidential.

The Data Protection Officer shall subsequently request a written statement from the controller responsible for the process, who shall provide his or her answer within 15 working days. The Data Protection Officer may then request to receive additional information from him or her or any other party within a further 15 working days.

The Data Protection Officer shall respond to the requester within two months from the date of the request. This period may be suspended until the Data Protection Officer has received from the requester the additional information deemed necessary.

Upon closure of the procedure the Data Protection Officer may make recommendations to the controller concerned. In case of a serious breach of Regulation (EC) 45/2001 by the controller, the Data Protection Officer shall immediately inform the Executive Director of the Agency thereof, who shall decide on the measures necessary.

No one shall suffer prejudice on account of a matter brought to attention of the Data Protection Officer. This procedure also does not prevent the data subject from addressing his or her complaint directly to the European Data Protection Supervisor under Article 33 or Regulation (EC) 45/2001.

3.1.12. Handling personal data breaches

Notification duty

In the case of a personal data breach, the controller shall without undue delay notify the personal data breach to the Data Protection Officer. Similarly, the Security Manager shall notify to the Data Protection Officer any security incident involving personal data.

A processor (i.e. external service provider) working for the Agency shall alert and inform the controller without undue delay after the establishment of a personal data breach.

The Data Protection Officer shall investigate also any incident that may involve a personal data breach whenever such incident is brought to his attention via any other channels and invite the controller to comment and, where appropriate, submit a data breach notification.

The notification to the Data Protection Officer shall at least contain the following information:

- (a) a description of the nature of the personal data breach, including the number of persons concerned, the number of data records concerned and the possible impact;
- (b) a contact point where more information can be obtained;
- (c) measures proposed or taken to mitigate possible adverse effects of the data breach;
- (d) measures proposed or taken to prevent similar data breaches in the future.

The information may if necessary be provided in phases.

Protection of Personal Data**Mitigating measures**

The controller, in consultation with the Data Protection Officer, shall without undue delay put in place the necessary mitigating measures to remedy the breach and limit the impact of possible adverse effects. Additionally, the controller shall without undue delay put in place measures to avoid that a similar breach takes place again in the future.

Such mitigating measures shall comply with all requirements for the confidentiality and security of the processing, as outlined in Articles 21-22 of Regulation (EC) No 45/2001. Where the processing takes place via electronic means, the controller shall as far as possible implement appropriate technological protection measures that render the data unintelligible to any person who is not authorised to access it (e.g. via data encryption).

The Data Protection Officer shall have access to all files and IT tools at request to investigate the circumstances of the case. He shall assess the severity of the incident and he may issue recommendations for improvement.

Based on the circumstances of the incident, the severity and the likely impact of the data breach, the Data Protection Officer may decide to inform the senior management of the Agency and/or involve them in the follow-up where needed. The Data Protection Officer may under the same conditions decide to inform and/ or consult with the European Data Protection Supervisor on the data breach.

When the personal data breach is likely to adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject, the controller shall communicate the personal data breach to the data subject without undue delay. The communication shall describe the nature of the personal data breach and contain at least the information contained in point (b), (c) and (d) above, as well as information about the rights of the data subject, including redress.

The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the Data Protection Officer that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Complaints

Anyone affected by a personal data breach by the Agency shall have the right to redress. This includes the right of filing a complaint with the Data Protection Officer (recommended first channel, see ED/32/2010), the European Data Protection Supervisor (see Article 33 of Regulation (EC) No 45/2001), the European Ombudsman (Article 228 TFEU) and legal action before the General Court (Article 263 TFEU).

Register

The Data Protection Officer shall keep a register of all personal data breaches in the Agency. This register shall document the data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. The documentation shall only include the information necessary for that purpose. Where appropriate, s/he shall also enter the data breach in the Non-Conformities (NC-CAPA) register. The Data Protection Officer shall report annually to the Executive Director on the data breaches notified.

3.1.13. Monitoring of compliance and enforcement

Internal:

The Data Protection Officer may, on his or her own initiative or at the request of the Agency, the controller, the Staff Committee or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller. Audits can be performed, alone or in cooperation with Agency's Internal Audit Capability (IAC).

The Data Protection Officer shall have access at all times to the personal data processed by the Agency and to all offices, data-processing installations and data carriers. Controllers shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions (Annex to Regulation (EC) 45/2001).

Moreover, the Data Protection Officer, in cooperation with the security team, may undertake inspections of the ECHA premises and of the ECHA networks to audit data protection compliance. Conclusions are shared with the Executive Director of the Agency and recommendations for improvement of practices are communicated to the controllers and to the staff of the Agency where applicable.

Despite having the competence to monitor compliance with the Regulation and to handle complaints, the Data Protection Officer has limited powers of enforcement. However, the Data Protection Officer has the possibility to bring to the attention of the Appointing Authority any failure to comply with the obligations under Regulation (EC) 45/2001 with a view to possible application of Article 49. Additionally he may refer any matter to the European Data Protection Supervisor, who may use his or her powers as foreseen in Article 47 of Regulation (EC) 45/2001.

External:

The European Data Protection Supervisor has the following monitoring and enforcement powers as foreseen in Article 47 of Regulation (EC) 45/2001:

- advise the data subjects in the exercise of their rights;
- refer a matter to the controller in the event of an alleged breach of data protection, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
- order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19 of Regulation (EC) 45/2001;
- warn or admonish the controller;
- order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of data protection and the notification of such actions to third parties to whom the data have been disclosed;
- impose a temporary or definitive ban on processing;
- refer a matter to the Executive Director of the Agency and, if necessary, to the European Parliament, the Council and the Commission;
- refer a matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;
- intervene in actions brought before the Court of Justice of the European Communities.

The European Data Protection Supervisor has the power to obtain access to all personal data and to all information necessary for his or her enquiries, as well as to any premises in which the Agency carries out its activities.

4. Flowchart

N/A

5. Definitions

Term or abbreviation	Definition
Controller	The unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data.
Data subject	Identified or identifiable natural person.
Personal data	Any information relating to an identified or identifiable natural person.
Personal data breach	All instances where personal data has been accidentally or unlawfully destroyed, lost, altered, disclosed without authorisation, accessed, transmitted, stored or otherwise processed.
Processing	Any operation or set of operations which is performed upon personal data, whether or not by automatic means.
Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

6. References

Associated document code	Document name
TFEU	Treaty on the Functioning of the European Union
Regulation (EC) No 45/2001	Regulation of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
ED/32/2010	Executive Director's decision regarding the tasks, duties and powers of the Data Protection Officer and the Data Controllers
MB/11/2008 final	Code of Good Administrative Behaviour for the Staff of the European Chemicals Agency in their relations with the public

7. Records

No	Record name
1	Inventory of personal data processing operations at ECHA
2	Register of notifications of personal data processing operations at ECHA
3	Register of complaints and personal data breaches

No	Record owner	Storage location	Security level	Comments
1	Data Protection Officer	SharePoint	Internal	
2	Data Protection Officer	SharePoint	Internal	
3	Data Protection Officer	SharePoint	Highly restricted	

8. Annexes

N/A

9. Change history

Revision	Changed section	Change description	Date
1	-	Initial document	21/12/2011
2	Mainly 3.1.12	Contents transferred to new template. Inclusion of procedure for personal data breaches. Other small updates.	29/01/2014