LEGAL DEPARTMENT

Groupe Verallia

Personal data breach notification

This procedure may be updated from time to time to take into account, where necessary, European regulatory changes.

Document version control :

Version	Date	Author	Verification	Approval	Subject
V1.0	15/02/2021	Idea	Idea	Idea	Creation

Contents

Introduction

The General Data Protection Regulation (GDPR) requires data controllers to notify the data protection authority (e.g. CNIL for France), and, depending on the degree of severity, the data subjects of certain security incidents constituting personal data breaches.

Compliance with this obligation requires, within Verallia, the setting-up of an organization to ensure the detection of such breaches, to assess their severity and implement appropriate measures to minimize the risks, reduce the impacts on the data subjects and to identify any useful action allowing to prevent the occurrence of new breaches.

1. Purpose of this procedure

This procedure aims at defining what to do in the event of a personal data breach and to identify responsibilities in order to allow the notifications required by the GDPR and to organize the traceability of personal data breaches.

This procedure is intended for all Verallia personnel (employees, temporary staff, trainees, etc.), as well as for the personnel of Verallia's service providers acting as data processors within the meaning of Article 28 of the GDPR and in this respect processing personal data on behalf of Verallia, as well as, in general, for any person who processes/holds personal data on behalf of Verallia (hereinafter referred to as the "**Personnel**").

2. Definitions/types of breaches

The notion of personal data breach is defined in Article 4, 12° of the GDPR as : « *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* »

A data breach is thus a security incident involving personal data (however, not every security incident is necessarily a personal data breach).

There are three main categories of personal data breaches :

- **Confidentiality breaches** : potential or actual access to personal data by persons other than those authorized to access it for a particular purpose (unauthorized access)
- **Data availability breaches** : accidental or unauthorized destruction, loss or alteration of personal data making the data inaccessible (loss of control over data access),
- **Data integrity breaches** : unauthorized or accidental alteration of personal data (unwanted modifications).

A personal data breach may occur for the following reasons:

- Loss/Theft of a means of communication;
- Erroneous business processes/human error/negligence in data processing/malicious intentional acts by internal or external actors;
- Poor security/technical failure

Examples:

- Loss of a laptop, USB drive

- Theft/destruction of equipment
- Access to the system given by mistake to the wrong person
- Sending an email to the wrong person
- Use of an unsecured communication channel to exchange sensitive personal data
- Access to personal data by employee outside the scope of its professional authorization
- Unauthorized disclosure of personal data
- Unauthorized use/contrary to the purposes of the information system
- Untidy paper documents left accessible to third parties
- Cyber attack (phishing, ransomware)
- System failure
- Lack of secure passwords on computers, devices or applications containing personal data

Important : for the purposes of this procedure, the term personal data breach refers **to both actual and suspected breaches.**

3. General responsibilities

Within each Verallia entity, Verallia Personnel, under the guidance and control of the Company Data Protection Coordinator ("**Company DPC**"), assists in the investigations and actions necessary to detect, process and contain any breach.

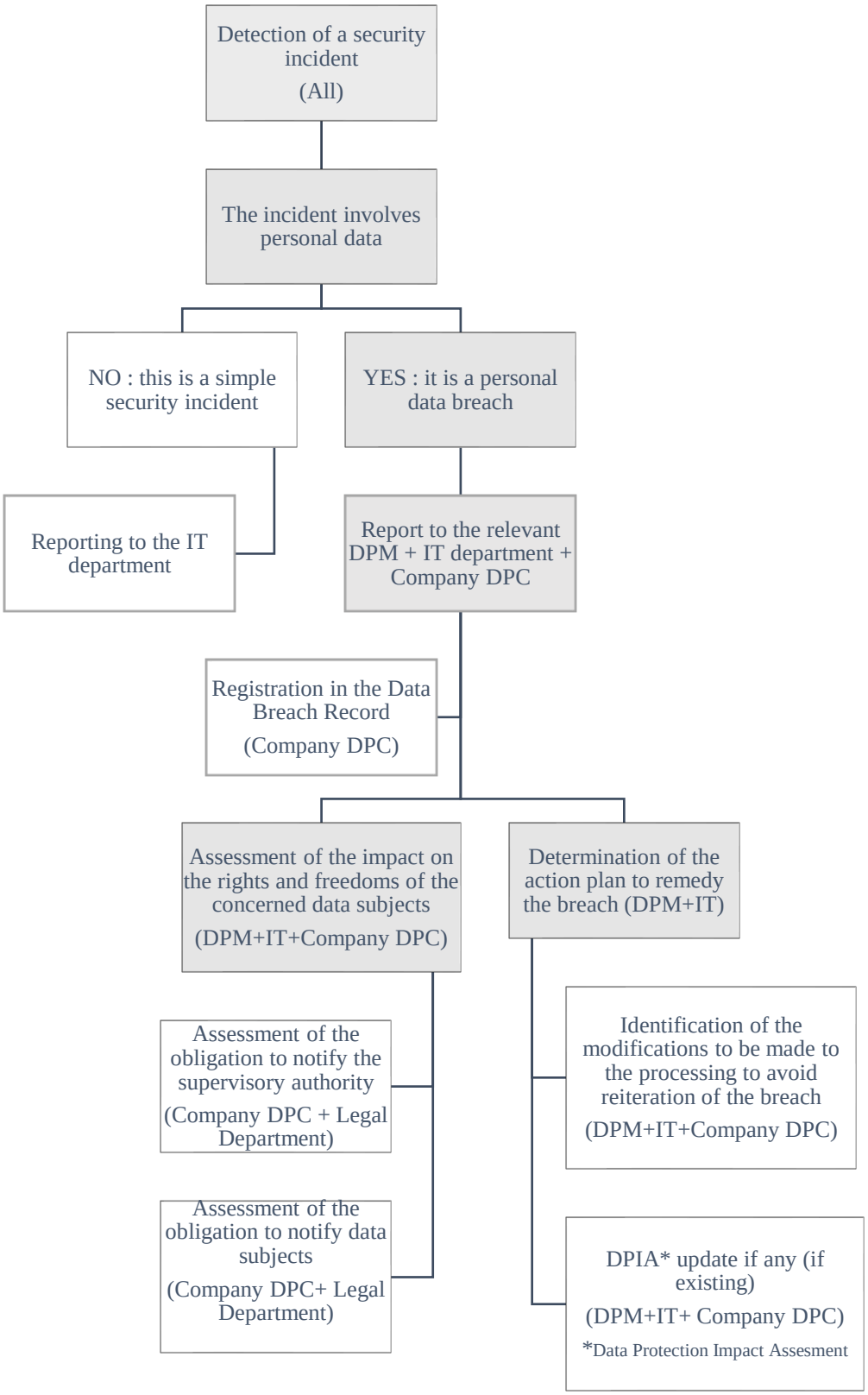
The Data Processing Managers ("**DPM**") and the Company DPC of each Verallia entity ensure the appropriate dissemination of and compliance with this procedure by the Personnel. They ensure that the Personnel assists in the investigations and actions necessary to address and contain the breach.

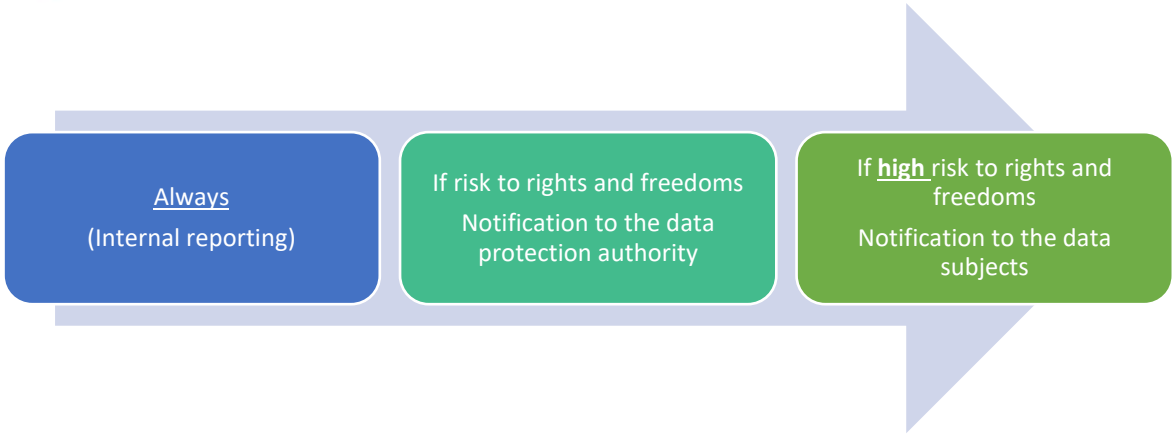
When the Company DPC is not a member of the Legal Department, the Company DPC is assisted by the Legal Department of the concerned Verallia entity (or, failing that, by the Group Legal Department).

In addition, the Company DPC includes in its annual report to the Group DPC a list of identified personal data breaches that have been notified to the supervisory authority and/or the concerned data subjects. In order to assist the Company DPC to make its report to the Group DPC, a template of report file may be found in the “Personal Data Protection” Sharepoint.

The concerned DPM and the IT department are responsible for the operational implementation of any action plan to address the breach with the assistance, if necessary, of the Company DPC (or Legal Department).

4. What to do ?


Detection of a security incident
(All)
The incident involves personal data
NO : this is a simple security incident
YES : it is a personal data breach
Reporting to the IT department
Report to the relevant DPM + IT department + Company DPC
Registration in the Data Breach Record
(Company DPC)
Assessment of the impact on the rights and freedoms of the concerned data subjects
(DPM+IT+Company DPC)
Determination of the action plan to remedy the breach (DPM+IT)
Assessment of the obligation to notify the supervisory authority
(Company DPC + Legal Department)
Identification of the modifications to be made to the processing to avoid reiteration of the breach
(DPM+IT+Company DPC)
Assessment of the obligation to notify data subjects
(Company DPC+ Legal Department)
DPIA* update if any (if existing)
(DPM+IT+ Company DPC)
*Data Protection Impact Assesment



5. Internal detection and reporting

Any person (the Personnel, including subcontractors[1]) must report in all cases and **without delay** to the concerned DPM as well as to the IT Department and Company DPC any breach of personal data, or any suspicion of breach of which he/she is aware in order to allow its processing as well as, if necessary, notification to the competent data protection authority (e.g. CNIL for France) within the deadlines required by the regulations (24 to 72 hours at the latest) and/or to the data subjects.

The report must include all known information regarding the circumstances of the breach, its significance, the type of personal data involved, etc. A form, a template of which is provided **in Appendix 1**, may be used by entities to assist in reporting.

Note: If the personal data breach is discovered after official working hours, the report should be made as soon as possible (as soon as the office open or on the next working day).

In case of processing:

Any processor of Verallia (within the meaning of the GDPR) must notify Verallia of any data breach as soon as possible after becoming aware of it.

It is therefore important that the contract between the processor and Verallia includes an obligation of the processor to do so on the part of the processor.

6. Evaluation of the breach

6.1. Breach and risk initial assessment

The concerned DPM, jointly with the IT Department and the Company DPC, conduct an initial assessment of the breach and its severity within the 24 hours following the breach.

The objective of this initial assessment is to contain the breach and preserve evidence.

Their action, as well as any action of any other person with expertise related to the breach (such as the processor), is to identify appropriate measures to determine the cause of the breach, assess the scale of the breach, and mitigate the potential harmful consequences, without destroying evidence that might be necessary to find the cause of the breach or to remedy it.

[1] *Article 33.2 GDPR*

6.2. Investigations and preliminary risk assessment

The concerned DPM, jointly with the IT Department and the Company DPC (with the support of the Legal Department) conducts the necessary investigations to assess the severity of the breach and the risks.

This assessment allows to determine whether the concerned Verallia entity is required to notify the breach to the competent data protection authority and, where applicable, to the concerned data subjects (see § 7) and, if so, to make the said notifications within the required deadlines, bearing in mind that :

- Notification to the competent authority is mandatory in case of risk to the rights and freedoms of the concerned data subjects
- Notification to individuals is mandatory in the event of a high risk to the rights and freedoms of the concerned data subjects

The **severity** of personal data breaches varies in terms of impact and risk to concerned data subjects **depending on the content, the amount of data involved, as well as the duration of exposure to the risk**. It is therefore important that the Verallia entity be able to identify the sensitivity of the data quickly and respond to all reported incidents quickly and in an appropriate manner.

The criteria to be considered are as follows:

- Type of breach
- Nature, sensitivity and volume of personal data
- Number of concerned data subjects
- Ease of identification of data subjects
- Severity of the consequences for the data subjects
- Vulnerability/special characteristics of data subjects
- Duration of exposure of the data

In the case of a proven breach, the risk assessment focuses only on the (real and/or potential) impact of the breach on the rights and freedoms of individuals.

The severity of the breaches can be classified as follows :

• Very high severity (major breach) : breach resulting in significant or irreversible consequences for the data subjects

Examples :

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft/ fraud/ damage to reputation
- financial loss
- unauthorized removal of pseudonymization
- loss of privacy
- any other significant economic or social disadvantage

• High severity (significant breach) : surmountable consequences but with serious difficulties (cost, important delay, aggravation of the situation) for the data subjects

- Medium severity (simple breach) : inconvenience for the data subjects

- Non-critical (minor breach) : simple inconvenience that people can easily overcome (e.g provide again their data)

Important: When assessing a risk, both the likelihood and the severity of the negative effect on the rights and freedoms of data subjects (i.e. impact on individuals) should be considered.

This assessment may evolve over time: some of the impact may be materialized as soon as the breach is detected, while others may occur later (for instance, in the case of stolen IDs, some of them may have already been used, while others may be used later).

At the end of this assessment, the Company's DPC, after consulting the Executive Management Team, the Legal Department (if different of the Company DPC) and the concerned business department, decides on the appropriate notification/information measures to be implemented (notification to the competent data protection supervisory authority, to the concerned data subjects, information to the police authorities, etc.) and, if so, the concerned DPM carries out the notifications with the support of the local Legal Department.

If notification mut be made to the CNIL (French data protection supervisory authority), any notification draft to the supervisory authority and/or to the data subjects concerned is sent to the Group Legal Department for advice.

If notification must be made to a data protection supervisory authority other than the CNIL, a copy of the notification is sent to the Group Legal Department for information.

6.3. Full evaluation

As soon as the breach is sufficiently identified and contained, and if the full assessment could not be completed within the notification timeframe, the concerned DPM and IT Department jointly conduct an in-depth assessment of the breach, the effectiveness of the given response, the overall impact on concerned data subjects, and any changes to the information system/organization that may be required to prevent further breaches.

7. External notification requirements

7.1. Notification to the competent data protection supervisory authority

The notification to the competent data protection supervisory authority must be made within the deadlines required by the applicable regulations**. In this regard, the GDPR provides that the notification must be made as soon as possible and, if possible, no later than 72 hours after becoming aware of the breach**. After this deadline, the controller (via the DPM with the support of the local Legal Department) must justify the reasons for the delay[2].

When the breach relates to a processor:

It is reminded that only Verallia (as data controller) may notify a data breach to the data protection supervisory authority : under no circumstances a processor of Verallia is authorized to notify in place of Verallia.

[2] *Article 33.1 GDPR. Please remind that vacation and/or week-ends are not reasons that can excuse delay for notification.*

Each entity must comply with the formalism required for notification. In France, notification is made through a dedicated secure teleservice accessible on the CNIL website: https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

Content of the notification (Article 33.3 GDPR[3]):

- The nature of the breach, including, if possible, the categories and approximate number of data subjects affected by the breach and the categories and approximate number of affected personal data records
- DPO contact details or, if there is no DPO, another point of contact's details from whom additional information can be obtained (it is recommended to provide the name of the CISO or Company DPC)
- The likely consequences of the data breach
- The measures taken or proposed to remedy the breach, including, if applicable, measures to mitigate any negative consequences

7.2. Notification to data subjects

Data subjects are informed, individually and as soon as possible[4], when the risk to their privacy is high (possibility of adjusting the information delivery time if the priority is to limit the risks of propagation).

Content of the notification (Article 34.2 GRPD), at a minimum and in clear and simple terms:

- The nature of the breach, including, if possible, the categories and approximate number of data subjects affected by the breach and the categories and approximate number of affected personal data records
- DPO contact details or, if there is no DPO, another point of contact's details from whom additional information can be obtained (it is recommended to provide the name of the CISO or Company DPC)
- The likely consequences of the data breach
- The measures taken or proposed to remedy the breach, including, if applicable, measures to mitigate any negative consequences

Exceptions to the notification obligation:

- When the breach in question is not likely to result in a risk to the rights and freedoms of natural persons
- When the controller has taken measures ensuring that the high risk to the rights and freedoms of the data subjects is unlikely to occur
- When the controller has implemented appropriate organizational and technical measures to the personal data affected by the breach (e.g. data encryption)
- When informing individuals would result in disproportionate efforts (in this case, public communication or a similar measure is used instead, allowing the data subjects to be informed in an equally effective manner).

8. Documentation to be kept

8.1. Data Breach Record

The Company DPC maintains a Data Breach Record (Article 33.5 GDPR) describing for each breach:

---

[3] Where it is not possible to provide all information at the same time, information may be provided in a phased manner without further undue delay
[4] Article 34.1 GDPR

- the nature of the breach;
- the categories and approximate number of individuals affected;
- the categories and approximate number of files affected;
- the likely consequences of the breach;
- the steps taken to remedy the breach and, where appropriate, to limit the adverse consequences of the breach;
- if applicable, the justification for not notifying the competent data protection supervisory authority or informing the data subjects.

All data breaches must be recorded in the data breach Record, regardless of whether they have been notified to the competent data protection supervisory authority or not.

A template of Record sheet may be found in the “Personal Data Protection” Sharepoint.

8.2. Other evidences

For each breach, the documentation to be maintained includes:

- The copy of the Data Breach Record sheet
- The action plan implemented to contain/address the breach
- The risk analysis conducted after the implementation of the remediation measures

If applicable:

- A copy of the notification to the relevant data protection supervisory authority and the acknowledgement of receipt
- A copy of the notifications made to data subjects

Appendix 1 : internal reporting form example

Reporting a personal data breach	
The breach is	☐ suspected ☐ proven ☐ in progress ☐ completed
Description of the breach	
Date and time the breach was discovered	
Date/period affected by the breach	
Name and position (employee, provider, resident...) of the person who identified the breach	
Name and contact details of the person reporting the breach (phone + email)	
Categories of persons likely to be impacted by the breach	
Categories of concerned personal data	
Categories of sensitive data	
Volume of data involved	
Cause/origin of the breach	
Processor involved/affected (if applicable)	
If the breach is ongoing, what actions are being taken to stop it?	
Initial assessment of the severity of the incident (impact for Verallia/potential consequences for the concerned data subjects)	
Any other relevant information	

Reserved for the Company DPC	
Date and time of receipt	