Valid for Organization	Information Type		
Volvo Group, AA10000	Instruction		
Issued by Function	Document ID		Information Class
Group Privacy Office, AA14110	0001-14-27269		Internal
Information Owner	Version	Reviewed Date	Page
Giraudon Guillaume	3.0	10/6/2020	1 (12)

0001-14-27269 Personal Data Breach Process

Table of Content

1. Definitions

Personal Data - any information which are related to an identified or identifiable natural person. The data can be in any type of form (i.e. electronic format, hard copy, structured or unstructured)

Personal Data Breach (PDB) – is defined in the *General Data Protection regulation* ("GDPR") and the *Act respecting the protection of personal information in the private sector* ("LP") as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, that exposes the rights and freedoms of the Data Subjects to risks. Indeed, where the processing of Personal Data may lead to physical, material, or non-material damage, there is a risk to the rights and freedoms of Data Subjects. Examples of damage include but are not limited to: identity theft, fraud, or financial damage; loss of confidentiality; Data Subjects becoming deprived of their right to exercise control over their Personal Data.

There are mainly three types of Personal Data Breaches:

- **[Availability breach]** Loss of access to, or destruction of personal data
  - Example: Personal Data lost due to accidents such as power outages or natural disasters (fire, floods).
- **[Integrity breach]** Alteration of personal data
  - Example: Employees salary information has been mismatched during a technical upgrade
- **[Confidentiality breach]** Unauthorised disclosure of or access to personal data
  - Examples:
    - An e-mail containing personal data has been sent to wrong recipients.
    - Personal data accessed through digital attacks by hackers
    - Stolen or lost laptops containing Personal Data

A personal data breach is an incident that is:

- Either **IT Security related** (e.g. cyber-attack or bug in an application)
- Or **Information Security related** (e.g. attachment containing Personal Data sent to the wrong department of an organization)

General reference to definitions in the Directive regarding Personal Data, has the same meaning in this instruction.

2. Scope and Purpose

This instruction applies to all the Group Volvo legal entities and to all individuals employed at the Volvo Group (including consultants or persons hired on a short-term contract basis) who process Personal Data.

This is an instruction of how to perform the Personal Data Breach process, based on the requirement on Data Breach in the GDPR and LP.

Detailed instructions and templates for main stakeholders are described further in this document.

Responsibilities and actions, in a Personal Data Breach context, vary depending on the role the company is acting: Data Controller or Data Processor.

3. Volvo Group's (and Nova Bus's) obligations

The Volvo Group and Nova Bus have the legal obligation to secure that personal data breaches are detected and managed in a timely and secure manner.

- Volvo Group and Nova Bus (**as Data Controller**) shall:
  - **Notify the Personal Data Breach to the Supervisory Authorities *('Commission d'accès à l'information'* in Québec) where applicable.**

- **GDPR (or LP) related PDB, shall be notified <u>within 72 hours</u>** post incident detection, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

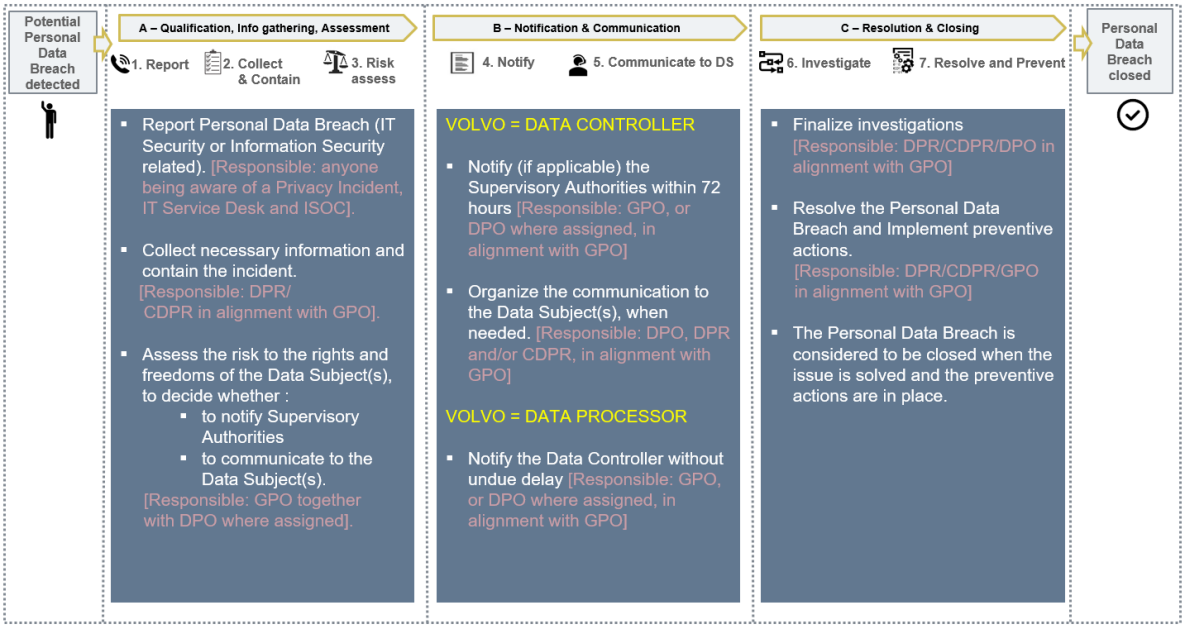
- When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, Volvo Group shall **communicate the personal data breach to the data subjects <u>without undue delay</u>**.

- Volvo Group and Nova Bus (**as Data Processor**) shall:
  - **Notify the Data Controller that a Personal Data Breach has occurred without undue delay.** This means that Data Processors are not obliged to communicate with Supervisory Authorities or Data Subjects. However, they are responsible to detect, assess, contain, investigate and resolve a Personal Data Breach and otherwise act upon the instructions of the Data Controller.

4. Personal data Breach process

The below is a general description of the Personal Data Breach process including process charts detailing the sequence of activities and deliverables, the responsibility for each activity. Further, for each activity a short description and instructions is given.

4.1. Outline of the overall process:



- **Process input:** The Personal Data Breach process is triggered when a <u>Potential Personal Data Breach is detected.</u>

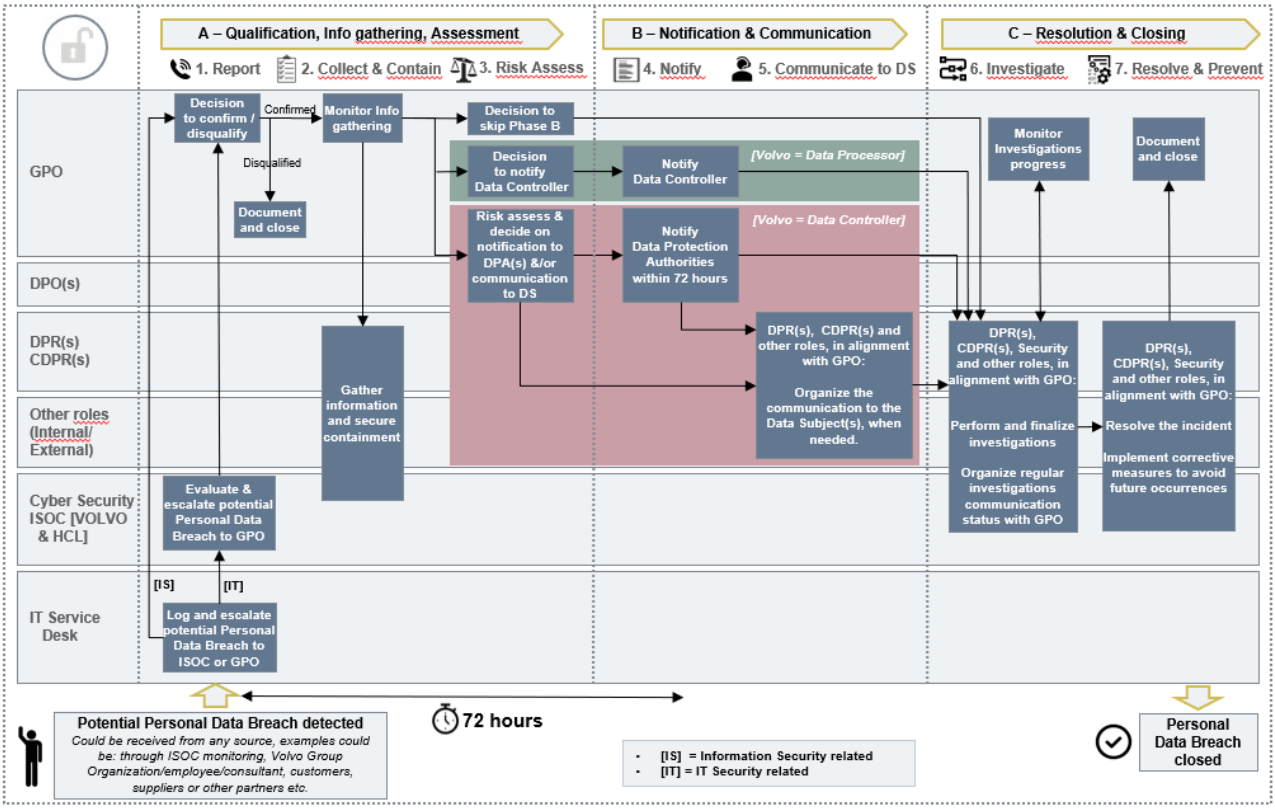
- **The process consists of 3 main phases:**
  - Process phase A – Qualification, Information gathering and Assessment
  - Process phase B – Notification and Communication
  - Process phase C – Resolution and Closing

- **Process output:** The Personal Data Breach process ends when the <u>Personal Data Breach is documented and closed</u>.

4.1.1. Important requirements:

- Confidentiality on data: The Personal Data Breach process handles personal data and it is essential to respect the confidentiality of each incident (data should only be shared with stakeholders in charge of the incident resolution)
- Act in a timely manner: As the Volvo Group or Nova Bus must notify DPAs within the stipulated timeframe (for GDPR 72 hours post incident detection, for LP, DPA must act 'with diligence') it is important to act swiftly. The incident should be assessed even though not all the information is known, to avoid delay in handling.

4.2. Detailed process



4.2.1. Process input: Potential Personal Data Breach detected

A Personal Data Breach can be detected through multiple sources:

- Either externally (from outside Volvo or Nova Bus) by an organization or an individual (ie: customer, supplier, a truck driver, a candidate…) acting either as Data Processor or as data Controller, public or private. Channels for receiving data breaches from external parties include commonly used means of communication such as telephone, email and/or online forms.
- Or internally (within The Volvo Group or Nova Bus) by an individual (e.g. employee or consultant) or through automatic/manual monitoring procedures (*).

(*): Volvo has internal processes in place to be able to detect and address a potential personal data breach. Cyber Security department in Volvo Group IT is responsible for setting adequate requirements on ISOC

(responsible for monitoring the IT environment of the Volvo Group) and Service Desk covering all aspects of IT security, including Personal Data Breaches.

4.2.2. Process phase A – Qualification, Information gathering and Assessment

4.2.2.1. Step 1: Report the Potential Personal Data Breach

A single way to report:

The IT Service Desk is the single point of reporting of all potential Personal Data Breaches. For Nova Bus, you must report all Breaches to the Data Protection Officer. In case a Personal Data Breach is reported to any other function than IT Service Desk this function should redirect it to the Service Desk in order to make sure that it is handled correctly according to the process.

Incident escalation path:

A potential Personal Data Breach is an incident that is:

- Either **IT Security related,** examples:
  - Bug in application resulting in disclosing data to unauthorized individuals
  - Personal data disclosed following a phishing email attack.
  - Personal Data has incorrectly been changed due to a technical upgrade
- or **Information Security related,** examples:
  - Mail containing personal data sent out to wrong recipients
  - Physical letter containing personal data shipped to the wrong recipient
  - Different kinds of surveys managed in a way so that personal data is disclosed to incorrect recipients.
  - Lost/Stolen IT equipment (Mobile/PC...) either unprotected or with likelihood that data has been accessed (credentials leaked)

The IT Service Desk (or Data Protection Officer) will register the incidents and escalate them either to **ISOC function** (when it comes to Personal Data Breaches that are **IT Security** related) or directly to the **Group Privacy Office** (when it comes to Personal Data Breaches that are **Information Security** related).

ISOC will manage Personal Data Breaches that are IT security related including containment, investigation and resolution. ISOC will also escalate, in a timely manner, all potential Personal Data Breaches (according to defined escalation principles) to the **Group Privacy Office** and provide all relevant information about the Personal Data Breach to enable the GPO and TD/BA/GF to proceed with the risk assessment.

Information to collect by the IT Service Desk when registering the incident:

The below information will help the Group Privacy Office in assessing the impact of the personal data breach and in the decision making whether to report to Data Protection Authorities.

- Personal Data breach description - *What has happened?*
- Personal data concerned – *What type of data has been disclosed?*
- Data Subject (DS) categories affected – *(employee, customer, driver, …)*
- Countries where DS are located (Sweden, France, Poland,…)
- Organizations concerned (HR, Finance, GTT, supplier, dealer,…)
- Detection date (And exact time) - *When was the incident detected?*
- Occurrence date - *When did the incident occurred?*
- How was it detected?

Decision to confirm/disqualify the incident

As soon as a potential Personal Data Breach is reported to the Group Privacy Office, a decision making is organized to:

- ✓ either disqualify the incident. In such case, the Group Privacy Office will document the incident and proceed with the closure.
- ✓ or confirm the incident, enabling the process to continue.

The above decision may not be possible straightaway, and the Volvo Group may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred.

4.2.2.2. Step 2: Collect information and contain the Personal Data Breach

Information gathering: For the Group Privacy Office to assess the incident properly, some key elements of information are required, for example:

- *Personal Data Breach description*
- *Personal data concerned*
- *Data Subject (DS) categories affected*
- *Countries concerned*
- *Legal entities concerned*
- *TD/BA/GF concerned*
- *Volvo role*
- *Detection date (and time - mandatory)*
- *Occurrence date*

The exhaustive list of information required is available in the following Personal Data Breach - Information gathering template . For Nova Bus, please use Data Privacy Officer's template.

In many cases, not all the information is known at first end and it is required to gather potential missing information. If necessary and as soon as a potential Personal Data Breach is confirmed, the Group Privacy Office liaises with the corresponding DPR/CDPR to kick-off the missing information gathering activity.
When all necessary information is available to the Group Privacy Office, the GPO will inform the corresponding DPR/CDPR.

Personal Data Breach containment: It is Volvo Group responsibility, regardless of its role (Data Controller or Data Processor), to take effective steps, to contain the Personal Data Breach in order to avoid further impact on the affected individuals.

The findings from the evaluation made by ISOC function shall serve as the initial basis for the containment decision making.

In order to manage and contain a Personal Data Breach, ISOC has launched a Security Incident Response Team "SIRT". The SIRT consists of relevant representatives from ISOC team (Volvo & HCL), Cyber Security (Volvo & HCL), GPO Office and other relevant stakeholders. The information gathered by SIRT will be communicated to the GPO on a regular basis. SIRT is also responsible for managing the technical and IT related aspects of handling, containing and solving the Personal Data Breach.

4.2.2.3. Step 3: Risk assess the Personal Data Breach

As soon that the GPO receives the necessary information related to a confirmed Personal Data Breach, the GPO, together with DPO where assigned, shall take the following steps depending on whether The Volvo Group (or Nova Bus) is acting as Data Controller or as Data Processor.

- **Volvo as Data Processor**

The Volvo Group (or Nova Bus), as Data Processor, shall, according to article 33 of the GDPR (article 3.5 (2), **notify the Data Controller without undue delay** (or with diligence in virtue of the LP) after becoming aware of a Personal Data Breach, which obligation is also reflected in the data processing agreement between the parties. The decisions whether to notify the Data Protection Authorities as well as whether to communicate to the affected Data Subjects is the responsibility of the Data Controller.
If and after notifying the Data Controller, The Volvo Group, as Data Processor, should carry on with activities from Phase C "Resolution & Closing".

- **Volvo as Data Controller**

The Volvo Group, as Data Controller, shall, according to article 33 of the GDPR (article 3.5 (2) LP, **risk assess the Personal Data Breach**, considering at first place, the likelihood and the potential severity of the impact on the Data Subject(s) whom Data have been affected.
This analysis will be key to determine:

- **Whether a notification to the supervisory authorities is required**
  - Supervisory Authorities are to be notified, unless it is unlikely that the Personal Data Breach will result in a risk to the rights and freedoms of the Data Subjects.
- **Whether a communication to the affected Data Subjects is necessary**
  - Affected Data Subjects are not to be informed about the incident unless the Data Breach is likely to result in a high risk to their rights and freedoms.

- **High risk**: This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation.

- **Likely:** When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, where personal aspects of the Data Subject are evaluated, such as work performance, economy, health, or personal preferences or interests; and where a large amount of personal data is processed such damage should be considered likely.

In cases where the GPO, together with the DPO where assigned, will decide neither to notify the Supervisory Authorities, nor to communicate to the Data Subjects, the Phase B "Notification & Communication" will be skipped and the process will carry on with Phase C "Resolution & Closing".

Following aspects are to be considered when assessing the risk:

- The type of breach (availability, confidentiality, integrity)
- The nature, sensitivity, and volume of personal data (e.g. a small amount of Sensitive Personal Data can have a high impact on the Data Subject)
- The ease of identification of individuals (direct identification or through matching of data)
- The severity of consequences for individuals (the more sensitive the data, the higher the risk of harm will be to the Data Subjects affected)
- Special characteristics of the individual (e.g. vulnerable, children etc.)
- The number of affected individuals (however, a Data Breach can have a severe impact on even one individual)
- Special characteristics of the Data Controller (e.g. Previa represents a high risk)
- Combination of the severity of the potential impact and the likelihood of these occurring

Risk assessment for each qualified Personal Data Breach is documented in the logging tool and in the following template: Personal Data Breach – Risk assessment template. For Nova Bus, please use templates prepared by Data Privacy Officer.

Conditions where notification is not required: Data Breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the Supervisory Authorities. An example might be where Personal Data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual.

Example: A breach that would not require notification to the Supervisory Authorities would be the loss of a securely encrypted mobile device, utilized by the Volvo Group and its staff. Provided the encryption key remains within the secure possession of the Volvo Group and this is not the sole copy of the Personal Data then the personal data would be inaccessible to an attacker. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of Data Subjects will change and thus notification may now be required.

Documentation
The risk assessment and final decision shall be documented by the GPO in writing in the Personal Data Breach logging tool centrally managed by the GPO. Templates can be found in the end of the present document. For Nova Bus, the decision shall be documented by the Data Privacy Officer in writing.

4.2.3. Process phase B – Notification and Communication

Activities handled in phase B are undertaken upon decisions made during the risk assessment of the Personal Data Breach (Phase A – Step 3) and those vary according to the role in which the Volvo Group or Nova Bus is acting on (Data Controller or Data Processor).

4.2.3.1. Step 4: Notify

- **Volvo or Nova Bus as Data Processor**

When acting as Data Processor, the Volvo Group shall notify the controller without undue delay after becoming aware of a personal data breach, which obligation is also reflected in the data processing agreement between the parties.

The notification shall:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of Group Privacy Officer, and/or Data protection Officer when applicable as well as any other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to contain and resolve the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The following template Personal Data Breach - Notification to Data Controller(s) is made available to support the notification to the Data Controller(s). For Nova Bus, please use form prepared by Data Protection Officer.

- **Volvo or Nova Bus as Data Controller**

When acting as Data Controller, the Volvo Group, through the GPO or DPO where assigned, shall without undue delay and not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Authority.

Being 'aware' requires a reasonable degree of certainty. After first being informed of a potential Personal Data Breach (internally or externally, proactively or reactivity), the Volvo Group may undertake a short period of investigation (Phase A – Step 1 – decision to confirm/disqualify), in order to establish whether or not a breach has in fact occurred. During this period of investigation Volvo may not be regarded as being “aware”. Initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place and the possible consequences for individuals; a more detailed investigation can then follow.

The Lead Authority for the Volvo Group is Datainspektionen in Sweden. However, depending on various factors such as the country(ies) where affected data subjects reside, the Personal Data Breach may be reported to another Data Protection Authority (ie: CNIL for a Personal Data Breach affecting Renault Trucks employees located in France). In Quebec, the Lead Authority is the ‘Commission de l’accès à l’information.’

In all cases, the decision to notify shall be taken jointly by the GPO and corresponding DPO (where assigned).

The notification to the Data Protection Authority should contain at least:

a) A description of the nature of the Data Breach;
b) The categories and number of concerned Data Subjects;
c) The categories and approximate number of Personal Data records concerned;
d) Contact information to the GPO, if applicable, or point of contact where more information can be obtained;
e) A description of the likely consequences of the Data Breach, and
f) A description of the measures taken or proposed to be taken by Volvo to address the Data Breach, including reasonable measures to mitigate the possible adverse effects of the Data Breach;
g) Indicate whether the breach involved establishments located in other Member States and in which Member States data subjects are likely to have been affected by the breach.
Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Where, and in so far as, it is not possible to provide at the same time all information related to the Personal Data Breach, this may be provided in phases without undue further delay.

4.2.3.2. Step 5: Communicate to the Data Subject(s)

This activity will only be handled in the case the Volvo Group is acting as Data Controller and when the personal data breach is likely to result in a high risk to the rights and freedoms of data subject(s), the DPO, DPR and/or CDPR, in alignment with GPO, shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the following information:

a) A description of the nature of the breach;
b) The name and contact details of the data protection officer or other contact point;
c) A description of the likely consequences of the breach; and
d) A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects; and

e) Provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords.

The need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

Depending on the circumstances, either a (i) direct communication to the data subjects, or (ii) public communication if individual notifications are considered disproportionate.

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media.

Communication is not required if:

- Volvo or Nova Bus (as Data Controller) has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.
- Volvo (as Data Controller) has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to previously is no longer likely to materialize.

4.2.4. Process phase C – Resolution and Closing

4.2.4.1. Step 6: Investigate

At this stage of the process, not all necessary information may have been gathered in order to resolve the Personal Data Breach, so an investigation may have to be carried out.

There will also be a need to decide how forensic the analysis should be and what information must be collected to support such analysis. This decision has a special importance if the data breach has a significant impact and/or is reported to the Data Protection Authorities.

DPR(s), CDPR(s), Security and other roles, are responsible to undertake these activities. Actions and decisions taken have to be handled in alignment with the GPO.

4.2.4.2. Step 7: Resolve and Prevent

In this step of the Personal Data Breach process, the DPR(s), CDPR(s), Security and other roles, in alignment with the GPO, will ensure that the incident is definitely resolved.

In order to prevent reoccurrence of the Personal data breach a detailed root cause analysis has to be made (DPR(s), CDPR(s), Security and other roles) in order to understand why the data breach could happen. Improvement actions have then to be triggered. A final report should also be provided to the GPO.

- In the case of an IT Security related Personal Data Breach, the ISOC function is responsible for resolving the Personal Data Breach and preventing it from re-occurring in accordance with the Incident Management Process.
- In the case of an Information Security Personal Data Breach, the GPO is responsible to monitor that the Personal Data Breach is resolved and that preventive actions are taken in order to minimize risk of the data breach to reoccur.

Following the finalization of the investigation the following issues should be considered by the GPO and other relevant stakeholders (DPO, DPR, CDPR, Security, …):

- Is there a need to take additional measures in terms of communication to data subjects, supervisory authorities or other involved or affected third parties?
- In case notifications were made to the Supervisory Authorities or information was provided to the affected data subjects, what were the reactions or consequences from such reports?
- To what extent should the handling of personal data be changed or updated, including relevant changes in processes or IT solutions, as a consequence of the actual or potential Data Breach?
- How well did the Data Breach process and related instructions function, any updates needed?

In some situations, there may be a need to evaluate the execution of the process in handling the Personal Data Breach. In such case, the GPO will conduct some lessons learned in order to identify the required improvements. The result of the analysis has to be documented centrally in the Personal Data Breach logging tool and GPO Office must secure the implementation of the identified improvements.

Regardless of whether or not a breach needs to be notified to the supervisory authority, Volvo must keep documentation of all breaches as outlined in the Data Breach logging tool on the Volvo Group Privacy Network Teamplace.

4.2.5. Process Output: Personal Data Breach closed

A Personal Data Breach is considered to be closed when both the incident is resolved, and the preventive actions are in place.

5. Roles and responsibilities:

ROLE	ACCOUNTABILITY & RESPONSIBILITY
GPO = Group Privacy Officer (GPO role description in VGMS)	• Accountable for the overall Personal Data Breach process in the Volvo Group. • Accountable for assessing Potential Personal Data Breach breaches, deciding whether notification to Data Protection Authorities (DPAs) and communication to Data-Subjects are necessary. Accountable that notifications are done to relevant DPA in stipulated timeframe, in alignment with DPO, where assigned. These activities are to be done in alignment with DPO where assigned.
DPO = Data Protection Officer (DPO role description in VGMS)	• Input to GPO on whether to notify the local Data Protection Authorities ('CAI'), related to a Personal Data Breach • Responsible to manage the actual notifications to the local Data Protection Authorities • Involved in the notification to the affected data subjects – if deemed necessary by GPO
DPR = TD/BA/GF Data Protection Representative (DPR role description in VGMS)	• Manage Personal Data Breach activities (issue understanding, collection of information, communication to Data-Subjects and monitor closure of mitigation measures), according to guidance from GPO.
CDPR = Country Data Protection Representative CDPR role description in VGMS:	• Act as a local contact point for Volvo Group for local data privacy issues in the country. • Provide support to GPO/DPO/DPR when it comes to data gathering, translation and any specific local understanding.
Other roles:	• Any other roles required in managing the Personal Data Breach properly, local legal counsels, HR representatives, IT solution responsible, Data Processor(s) representatives (Customer, Supplier…)

ISOC = Information Security Operations Center (Cyber Security function hosted in both the Volvo Group and HCL)	• responsible for monitoring the IT environment of the Volvo Group. • Accountable for identifying and escalating personal data breach incidents to GPO. Also accountable for containing, investigating and resolving personal data breach incidents from a technical perspective.
IT Service Desk	• Accountable for escalating potential Personal Data Breach and escalating them (without undue delay) to either ISOC (IT Security related) or GPO (Information Security related). Service Desk is managed by HCL.

6. Overview of templates used in the PDB process

List of links to templates:

- Personal Data Breach - Information gathering template (Please use Data Privacy Officer template.)
- Personal Data Breach – Risk assessment template (Please use Data Privacy Officer template.
- Personal Data Breach – Information to supplier(s)
- Personal Data Breach - Notification to Data Controller(s)
-

7. Overview of appendices to this instruction

The following appendices are published to support this instruction:

- APPENDIX A. Checklist for GPO Office

8. References

- Directive regarding Personal Data

9. Version History

Date	Description of change
2020-10-07	First publication in VGMS