Data Privacy – Data breach incident

Process how to handle privacy data breach incidents

Version	0.2 - Draft	Last update	15/05/2018
Owner	Legal	Pages	
Source	InfoSec > public documents > initiatives > GDPR in IT > Data breach		

1 Introduction

- The General Data Protection Regulation (the GDPR) introduces the requirement for a Personal Data Breach (henceforth "Breach") to be notified to the competent national supervisory authority and, in certain cases, communicate the Breach to the individuals ("Data Subject") whose Personal Data (Art.4 (1) GDPR) have been affected by the Breach.
- This process describes
  - How to report a Breach
  - How to assess the impact
  - Who must be informed
  - How to contain and remediate the damage
  - The data privacy contact

1.1 Definition of a Breach

- One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, Personal Data shall be processed in a manner to ensure the appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- A "Personal Data Breach" persuant to Art 4(12) GDPR is given if:

> 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 Breach can include, but is not limited to,

- access to personal data by an unauthorised third party
- sending personal data to an unintended recipient
- lost or stolen computing devices containing personal data
- unauthorised destruction
- existence in a form that is no longer of any use to the Controller (Art.4 (7) GDPR)
- alteration of personal data
- corrupted or no longer complete personal data
- total loss of availability of personal data
- lost control or access by a Controller to existing personal data

1.2 Notification to the supervisory authority

In case of a Breach, the Controller must not later than 72hours after having become aware of it, notify the Breach to the supervisory authority unless the Breach is unlikely to result in a risk to the rights and freedoms of natural persons (Art.33(1) GDPR).

The competent authority is the national supervisory authority in the territory of the concerned Member State of the European Union to whom the performance of the tasks and the exercise of the powers conferred on it in accordance with the GDPR has been assigned to.

1.3 Notification to the concerned Data Subject

The concerned Data Subject has to be informed immediately if the Breach is likely to result in a high risk to the rights and freedoms of ther natural person (Art.34 (1) GDPR).

1.4 When to use this incident process

- This process describes how to act in case of a Breach where a Constellium legal entity is the Controller or in case a supplier (serving as a data Processor (Art.4 (8) GDPR), who is acting on behalf of Constellium, reports a Breach of Personal Data where Constellium is the Controller.

2 Trigger

- Constellium employees, contractors or suppliers who became aware of a Breach can start this process.

3 Owner

- This process is owned by the legal department of Constellium.

4 Procedure

4.1 Reporting an Data Privacy incident

Everybody who detects Breach must report the incident immediatelly to their data privacy contacts (appendix 1). The incident should be described by using appendix 2 “Data Privacy incident questionaire (part 1)” which needs to be filled in by the person who detected the incident prior to forwarding the report to the data privacy contact as defined in appendix 1.

The data privacy contact responsible of the affected Constellium legal entity (see contact list in appendix 1) acts as the Incident Manager for this case. The Incident Manager coordinates all required activities within Constellium until the incident is closed.

Actions to be performed per incident:

- assess the impact by using appendix 3: “Data Privacy – Incident questionaire (part 2 – to be answered by the Incident Manager)”

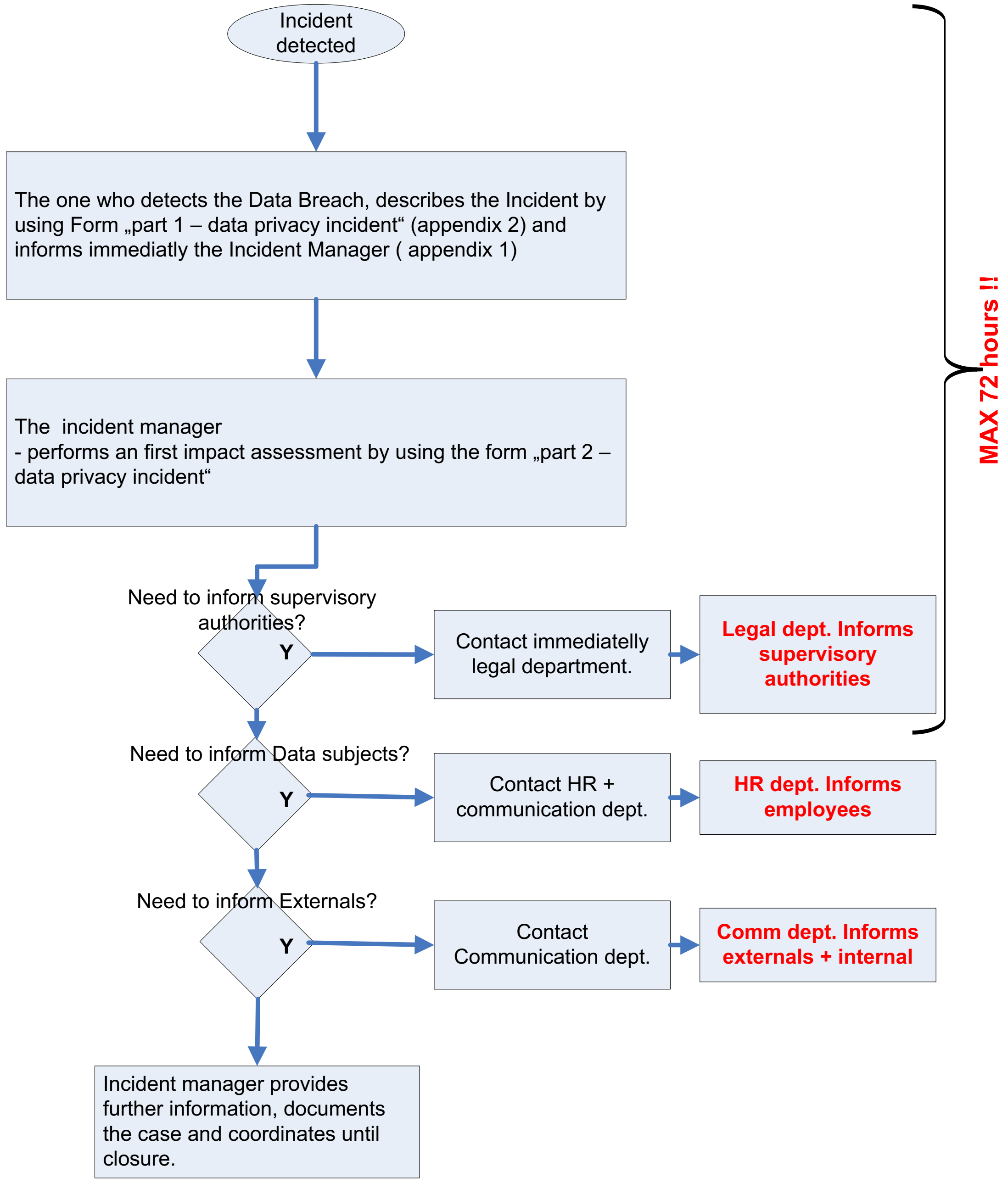
- determine if there is a need to inform the supervisory authorities.(Information must be done latest 72 hours after the incident was detected). The information of the competent supervisory authority shall be made by the Legal Department which needs to be informed respectively and provided with any and all documents and informations by the Incident Manager.
- Inform management about the incident and provide periodically status updates.
- determine if there is a need to inform affected Data Subjects (employees, customers, etc). The information of the affected Data Subject shall be made by the responsible HR Department which needs to be informed respectively and provided with any and all documents and informations by the Incident Manager.
- determine together with senior management if a public information should be done. The information to Public shall be made by the responsible Communications Department which needs to be informed respectively and provided with any and all documents and informations by the Incident Manager.

4.2 Documentation

The incident manager is in charge to document all steps, actions and remediation activities in order to evidence the proper handling of the incident.

4.3 Workflows

Data Privacy: Breach Workflow



Incident detected

The one who detects the Data Breach, describes the Incident by using Form „part 1 – data privacy incident“ (appendix 2) and informs immediatly the Incident Manager (appendix 1)

The incident manager
- performs an first impact assessment by using the form „part 2 – data privacy incident“

Need to inform supervisory authorities?

Y

Contact immediatelly legal department.

Legal dept. Informs supervisory authorities

MAX 72 hours !!

Need to inform Data subjects?

Y

Contact HR + communication dept.

HR dept. Informs employees

Need to inform Externals?

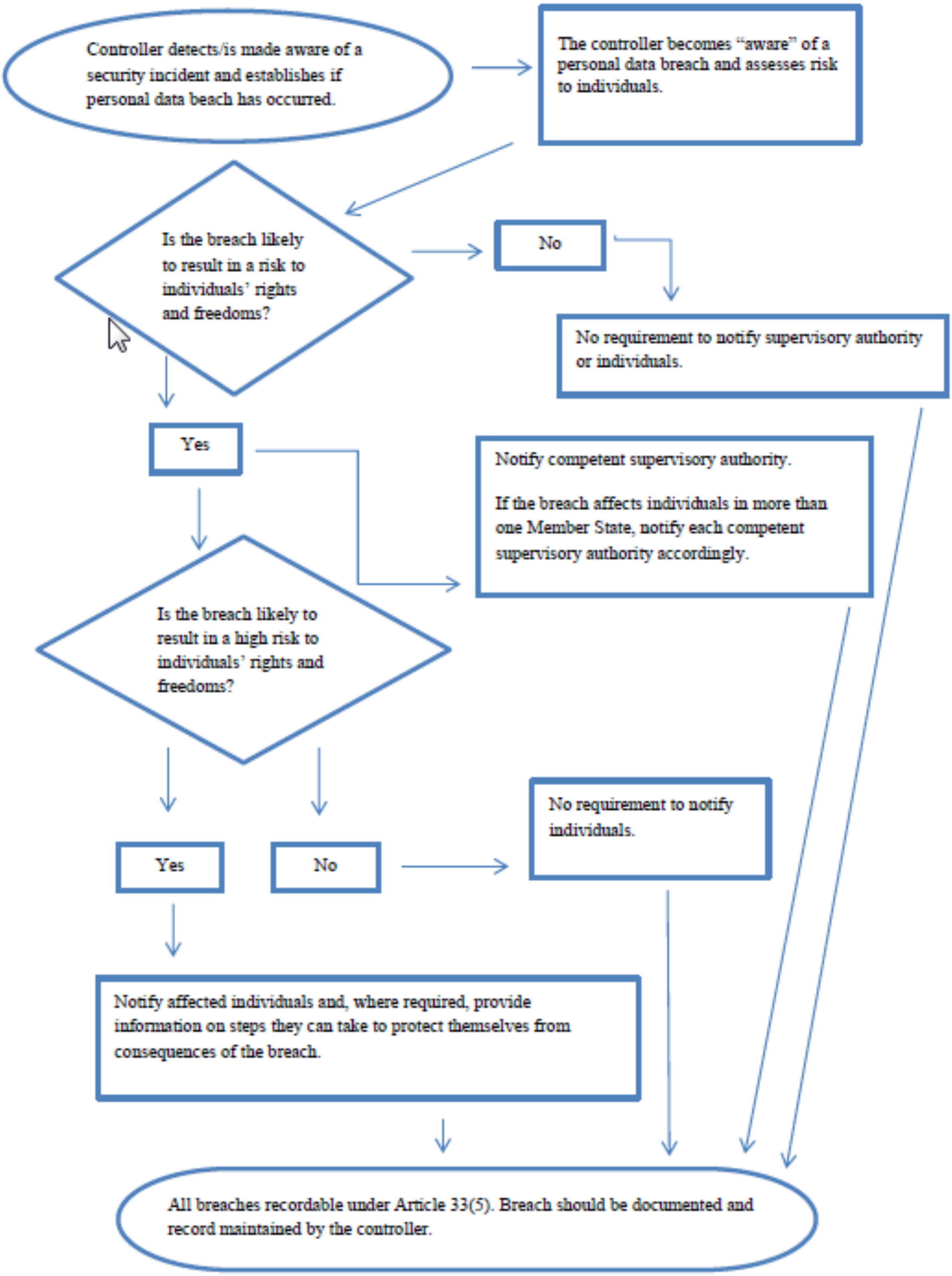
Y

Contact Communication dept.

Comm dept. Informs externals + internal

Incident manager provides further information, documents the case and coordinates until closure.

A. Flowchart showing notification requirements



Controller detects/is made aware of a security incident and establishes if personal data beach has occurred.

The controller becomes "aware" of a personal data breach and assesses risk to individuals.

Is the breach likely to result in a risk to individuals' rights and freedoms?

No

No requirement to notify supervisory authority or individuals.

Yes

Notify competent supervisory authority.

If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly.

Is the breach likely to result in a high risk to individuals' rights and freedoms?

Yes

No

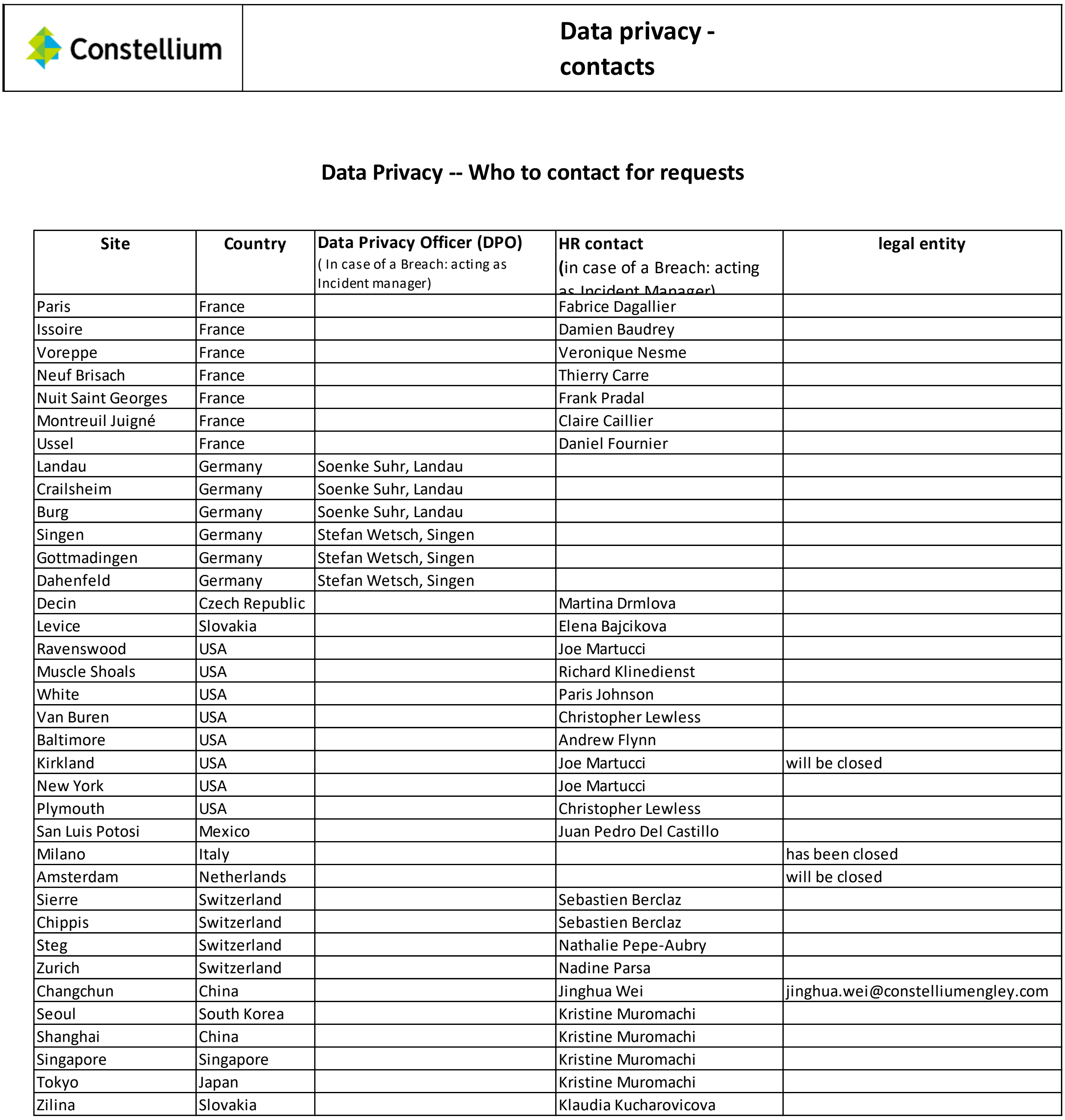
No requirement to notify individuals.

Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.

All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.

5 Appendixes:

5.1 Appendix 1: contact list:



Constellium

Data privacy - contacts

Data Privacy -- Who to contact for requests

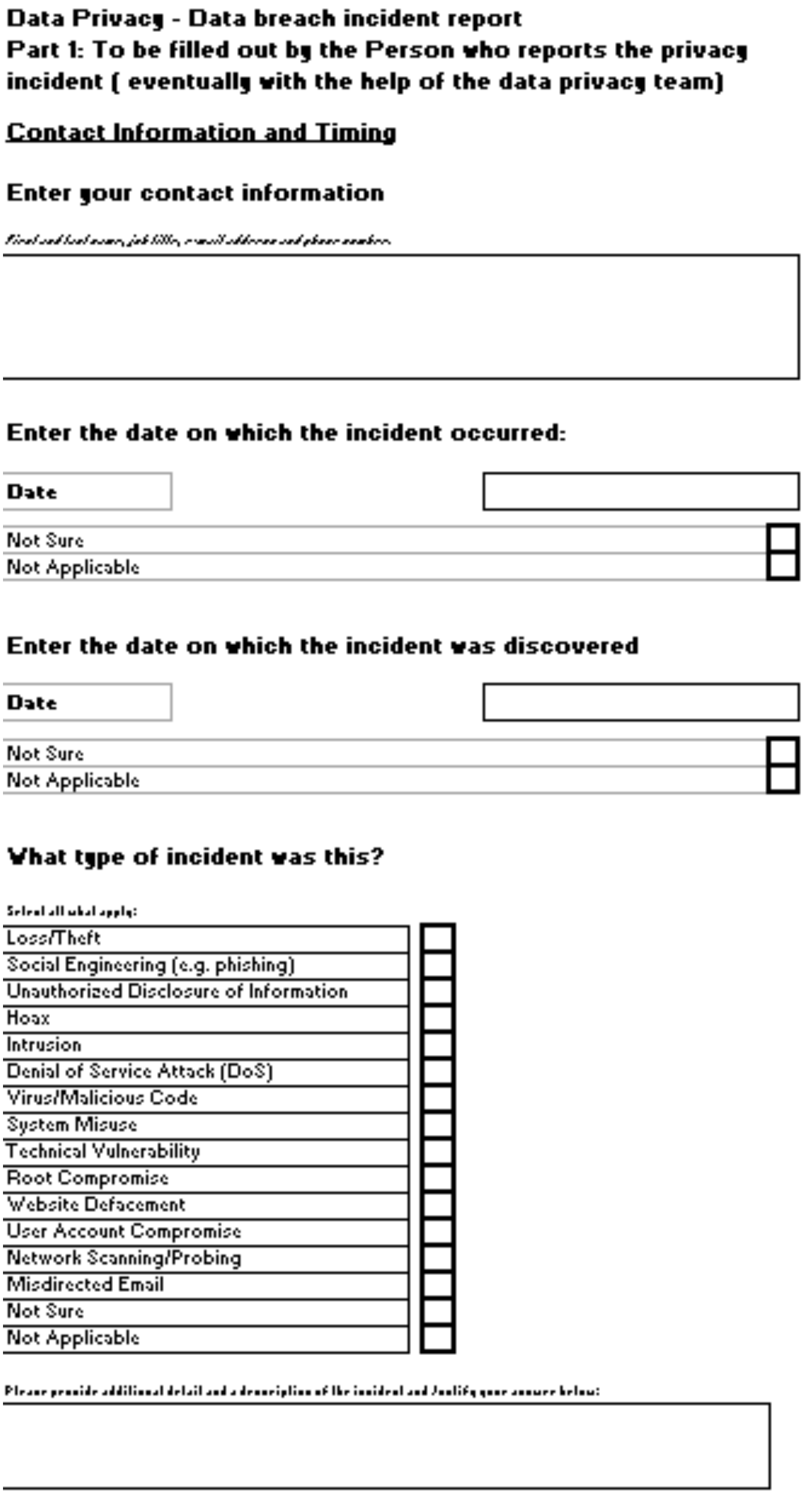
Site	Country	Data Privacy Officer (DPO) (In case of a Breach: acting as Incident manager)	HR contact (in case of a Breach: acting as Incident Manager)	legal entity
Paris	France		Fabrice Dagallier	
Issoire	France		Damien Baudrey	
Voreppe	France		Veronique Nesme	
Neuf Brisach	France		Thierry Carre	
Nuit Saint Georges	France		Frank Pradal	
Montreuil Juigné	France		Claire Caillier	
Ussel	France		Daniel Fournier	
Landau	Germany	Soenke Suhr, Landau		
Crailsheim	Germany	Soenke Suhr, Landau		
Burg	Germany	Soenke Suhr, Landau		
Singen	Germany	Stefan Wetsch, Singen		
Gottmadingen	Germany	Stefan Wetsch, Singen		
Dahenfeld	Germany	Stefan Wetsch, Singen		
Decin	Czech Republic		Martina Drmlova	
Levice	Slovakia		Elena Bajcikova	
Ravenswood	USA		Joe Martucci	
Muscle Shoals	USA		Richard Klinedienst	
White	USA		Paris Johnson	
Van Buren	USA		Christopher Lewless	
Baltimore	USA		Andrew Flynn	
Kirkland	USA		Joe Martucci	will be closed
New York	USA		Joe Martucci	
Plymouth	USA		Christopher Lewless	
San Luis Potosi	Mexico		Juan Pedro Del Castillo	
Milano	Italy			has been closed
Amsterdam	Netherlands			will be closed
Sierre	Switzerland		Sebastien Berclaz	
Chippis	Switzerland		Sebastien Berclaz	
Steg	Switzerland		Nathalie Pepe-Aubry	
Zurich	Switzerland		Nadine Parsa	
Changchun	China		Jinghua Wei	jinghua.wei@constelliumengley.com
Seoul	South Korea		Kristine Muromachi	
Shanghai	China		Kristine Muromachi	
Singapore	Singapore		Kristine Muromachi	
Tokyo	Japan		Kristine Muromachi	
Zilina	Slovakia		Klaudia Kucharovicova	

appendix 1 - data privacy - contacts.xl [Link to the file](#)

5.2. Appendix 2: data privacy – Breach incident report part 1 Link

to be filled out by the person who detected the breach

Data Privacy -
Incident questionair



Data Privacy - Data breach incident report
Part 1: To be filled out by the Person who reports the privacy incident (eventually with the help of the data privacy team)

Contact Information and Timing

Enter your contact information

First and last name, job title, e-mail address and phone number.

Enter the date on which the incident occurred:

Date		
Not Sure		□
Not Applicable		□

Enter the date on which the incident was discovered

Date		
Not Sure		□
Not Applicable		□

What type of incident was this?

Select all that apply:

Loss/Theft	□
Social Engineering (e.g. phishing)	□
Unauthorized Disclosure of Information	□
Hoax	□
Intrusion	□
Denial of Service Attack (DoS)	□
Virus/Malicious Code	□
System Misuse	□
Technical Vulnerability	□
Root Compromise	□
Website Defacement	□
User Account Compromise	□
Network Scanning/Probing	□
Misdirected Email	□
Not Sure	□
Not Applicable	□

Please provide additional detail and a description of the incident and Justify your answer below:

5.3. Appendix 3: data privacy – Breach incident report part 2 Link

To be filled out by the incident manager

Data Privacy -
Incident questionair

Data Privacy - Data breach incident report

Part 2: To be filled out by the Incident manager

At the time when the incident occurred, was our organization carrying out the processing affected by the incident on behalf of someone else (i.e. the "data controller")?

Yes	□
No	□
Not sure	□
Not applicable	□

Comments

A "data controller" is the party whom you are carrying out the processing on behalf of. The controller determines the purposes and means of the processing of personal data.

Based on your assessment of the responses in Part 1 - Threshold, do you consider the personal data breach to be likely to result in a high risk to the rights and freedoms of natural persons?

Yes	□
No	□
Not applicable	□

Comments

"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay." (GDPR, Article 34(1))

Would notification of data subjects involve disproportionate effort? Please explain.

Yes	□
No	□
Not applicable	□

Comments

Under Article 34(3)(c) of the GDPR, notification of data subjects is not required if "it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

explanation

What are the likely consequences to affected data subjects?

select all that applies:

5.4. Appendix 4: List of the National Data Protection authorities Link

20180419_National DataProtectionAuth

6 Document Revision

Author	**Version**	**Date**	**Change**	**Approval**
Dieter Knobelspies Claudia Blaesi	0.1 0.2	26/04/2018 15/05/2018	Initial version Storage location reviewed by Legal	