Bird & Bird & Enough uncertainty on data breaches!

Gabriel Voisin (Partner)
Simon Assion (Counsel)
20 April 2021

What are we going to cover today?

- Refresher on the current European breach notification landscape

- Juicy breach examples in the draft EDPB guidelines
  - Credential stuffing attack
  - Accidental transmission of data to a trusted third party
  - Stolen material storing non-encrypted personal data
  - Email exfiltration

- Top tips and best practices to be ready when an incident comes up

Refresher on the current European breach notification landscape

Bird & Bird

Refresher on the current European breach notification landscape

European wide sectorial breach obligations, e.g.
- NIS/Cyber security directive
- ePrivacy Directive
- PSD II
- EIDAS Regulation

Potential national sectorial breach obligations, e.g.
- Listed organisations
- Health organisations
- Gambling organisations

Bird & Bird

GDPR personal data breach notification obligations (1)

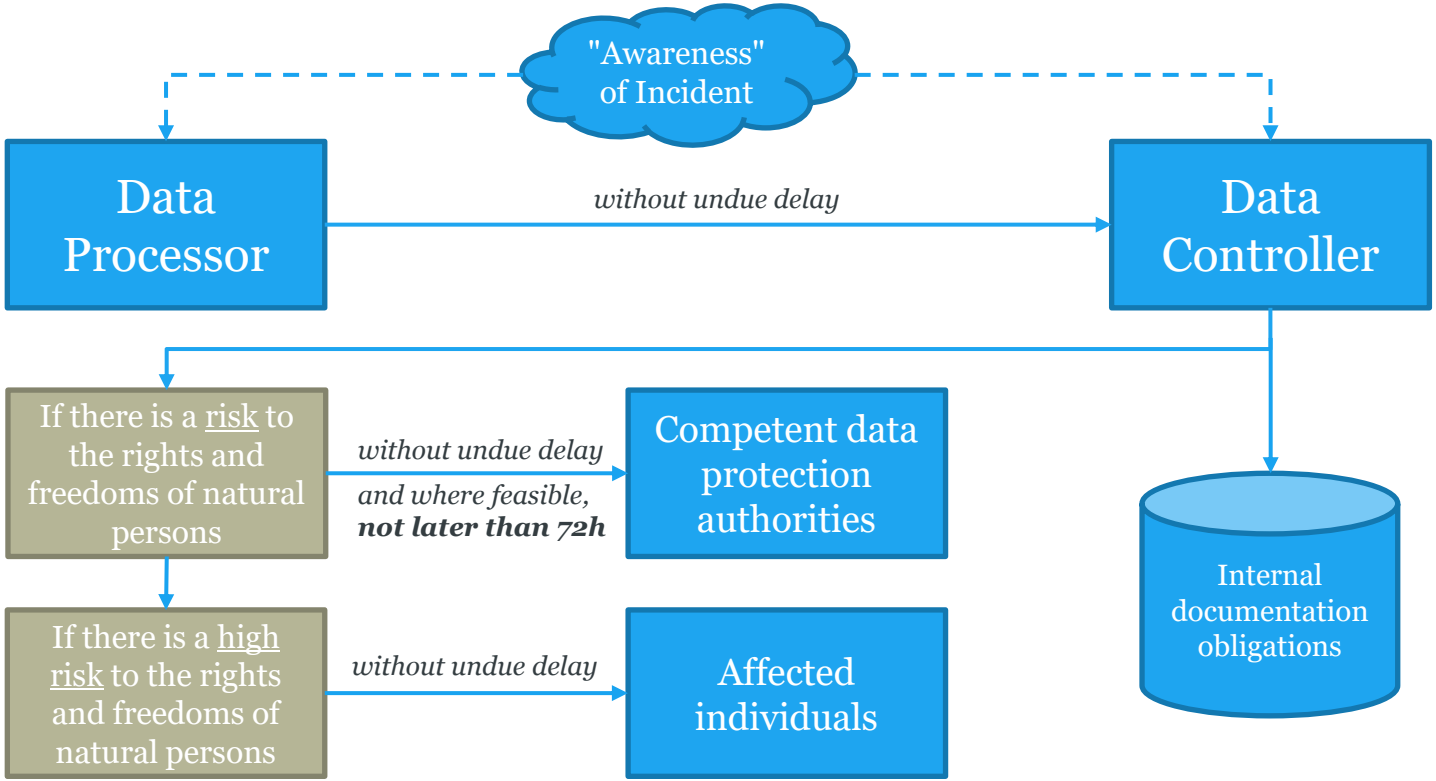
GDPR defines a "personal data breach" in Article 4(12) as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"

There are 3 types of personal data breaches:

- **Confidentiality** breach - where there is an unauthorised or accidental disclosure of, or access to, personal data
- **Integrity** breach - where there is an unauthorised or accidental alteration of personal data
- **Availability** breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data

Bird & Bird

GDPR personal data breach notification obligations (2)

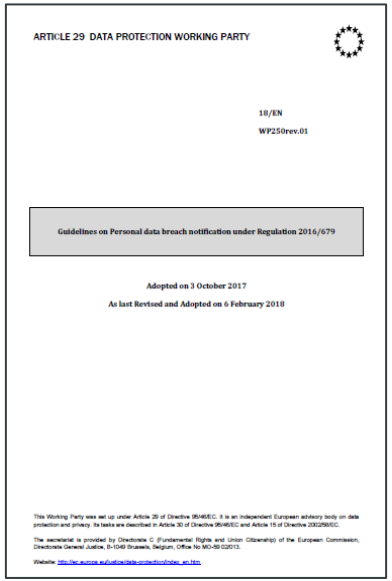


Bird & Bird

Juicy breach examples in the draft EDPB guidelines

Bird & Bird

EDPB guidelines on personal data breaches


ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN
WP250rev.01

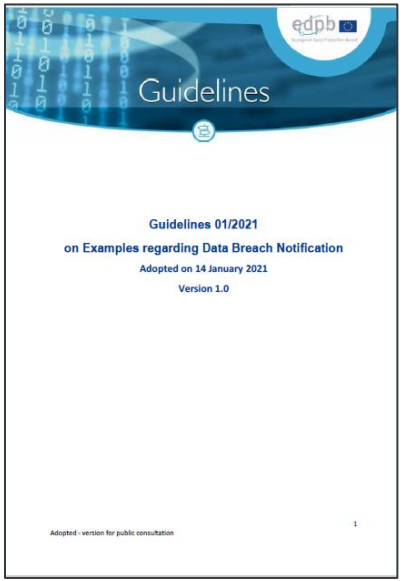
Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017
As last Revised and Adopted on 6 February 2018

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm



- Public consultation ended in March
- 32 contributions received
- Final version of the guidelines expected this year

Guidelines on Personal data breach notification under Regulation 2016/679 (last updated in 02/2018)

Draft Guidelines 01/2021 on Examples regarding Data Breach Notification

Bird & Bird

Juicy breach examples in the draft EDPB guidelines

RANSOMWARE

- CASE 1: Ransomware with proper backup and without exfiltration
- CASE 2: Ransomware without proper backup
- CASE 3: Ransomware with backup and without exfiltration in a hospital
- CASE 4: Ransomware without backup and with exfiltration

DATA EXFILTRATION ATTACKS

- CASE 5: Exfiltration of job application data from a website
- CASE 6: Exfiltration of hashed password from a website
- CASE 7: Credential stuffing attack on a banking website

INTERNAL HUMAN RISK SOURCE

- CASE 8: Exfiltration of business data by a former employee
- CASE 9: Accidental transmission of data to a trusted third party

LOST OR STOLEN DEVICES AND PAPER DOCUMENTS

- CASE 10: Stolen material storing encrypted personal data
- CASE 11: Stolen material storing non-encrypted personal data
- CASE 12: Stolen paper files with sensitive data

MISPOSTAL

- CASE 13: Snail mail mistake
- CASE 14: Sensitive personal data sent by mail by mistake
- CASE 15: Personal data sent by mail by mistake
- CASE 16: Snail mail mistake

OTHER CASES - SOCIAL ENGINEERING

- CASE 17: Identity theft
- CASE 18: Email exfiltration

Credential stuffing attack (case 7)

A bank suffered a cyber-attack against one of its online banking websites. The attack aimed to enumerate all possible login user IDs using a fixed trivial password. The passwords consist of 8 digits. Due to a vulnerability of the website, in some cases information regarding data subjects (name, surname, gender, date and place of birth, fiscal code, user identification codes) were leaked to the attacker, even if the used password was not correct or the bank account not active anymore. This affected around 100.000 data subjects. Out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker. After the fact, the controller was able to identify all illegitimate log-on attempts. The data controller could confirm that, according to antifraud checks, no transactions were performed by these accounts during the attack. The bank was aware of the data breach because its security operations centre detected a high number of login requests directed toward the website. In response, the controller disabled the possibility to log in to the website by switching it off and forced password resets of the compromised accounts. The controller communicated the breach only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed.

Internal documentation	Notification to DPA	Communication to affected individuals
YES	**YES**	**YES**

Case 7: A change from certain DPAs' previous practices

- The French DPA (CNIL) for instance had a different line on this (until recently)
- In the past, in case of credential stuffing attacks where the credentials are only tested and there was no evidence of further misuse, controllers were told to:
  - notify the affected individual within a period not exceeding 72 hours
  - force the affected individual to change his password next time he logs in
  - recommend the affected individual to change his password if used in the context of other services
- By contrast, the CNIL did not expect to be notified about this kind of incident. Source: https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
- The draft EPDB example lowers the bar here and if confirmed would require alignment with your IT/IS teams

Accidental transmission of data to a trusted 3rd party (case 9)

An insurance agent noticed that – made possible by the faulty settings of an Excel file received by e-mail – he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. The arrangement between the data controller and the insurance agent obliges the agent to signal a personal data breach without undue delay to the data controller. Therefore, the agent instantly signalled the mistake to the controller, who corrected the file and sent it out again, asking the agent to delete the former message. According to the above-mentioned arrangement the agent has to confirm the deletion in a written statement, which he did. The information gained includes no special categories of personal data, only contact data and data about the insurance itself (insurance type, amount). After analysing the personal data affected by the breach the data controller did not identify any special characteristics on the side of the individuals or the data controller that may affect the level of impact of the breach.

Internal documentation	Notification to DPA	Communication to affected individuals
YES	NO	NO

Case 9: A welcome confirmation of an existing use case

- The 2018 Guidelines on Personal data breach notification already contained an example along this line:

Where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals.

- The use of the words "trusted parties" suggests that this would cover *controller to processor* but also *controller to controller* situations

Stolen material storing non-encrypted personal data (case 11)

The electronic notebook device of an employee of a service provider company was stolen. The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers. Due to the unavailability of the stolen device it was not possible to identify if other categories of personal data were also affected. The access to the notebook's hard drive was not protected by any password. Personal data could be restored from daily backups available.

Internal documentation	Notification to DPA	Communication to affected individuals
YES	**YES**	**YES**

Case 11: Replace the words 'notebook' by 'mobile phone' and you can imagine the drama…

- In order not to have to notify competent DPA(s) and affected individuals, controllers will need:
  - adequate and active password protection at device level
  - back-up of the data stored on the device
  - capacity to remotely wipe out the content of the device after being reported missing/stolen
- This is likely to require conversations with IT/IS/facility teams

Email exfiltration (case 18)

A hypermarket chain detected, 3 months after its configuration, that some email accounts had been altered and rules created so that every email containing certain expressions (e.g. “invoice”, “payment”, “bank wiring”, “credit card authentication”, “bank account details”) would be moved to an unused folder and also forwarded to an external email address. Also, by that time, a social engineering attack had already been performed, i.e., the attacker, posing as a supplier, had had that supplier bank account details altered into his own. Finally, by that time, several fake invoices had been sent that included the new bank account detail. The monitoring system of the email platform ended up giving an alert regarding the folders. The company was unable to detect how the attacker was able to gain access to the email accounts to begin with, but it supposed that an infected email was to blame for giving access to the group of users in charge of the payments. Due to the keyword-based forwarding of emails, the attacker received information on 99 employees: name and wage of a particular month regarding 89 data subjects; name, civil status, number of children, wage, work hours and remainder information on the salary receipt of 10 employees whose contracts were ended. The controller only notified the 10 employees belonging to the latter group.

Internal documentation	Notification to DPA	Communication to affected individuals
YES	YES	YES

Top tips and best practices to be ready when an incident comes up

Bird & Bird

Useful technical and organisational measures in the draft EDPB guidelines

In response to its 18 use cases, the draft EDPB guidelines provide a series of technical and organisational measures to prevent or limit the risks caused by personal data breaches, see:

- Page 13
- Page 18
- Page 21
- Page 25
- Page 29

Convert them into check lists and use them as a basis for a conversation with your organisation's IT/IS teams:

Bird & Bird

Design your checklist to serve as an *aide memoire* when you receive a breach call/email

- Is the incident a personal data breach?
- Are you acting as a data processor or a data controller?
- Do the NIS Directive or other breach notification law apply?
- When did the incident happen? When did you become "aware" of the incident?
- Where did the incident happen? Where are the data subjects located?
- What investigations have taken place so far? Has the incident been contained?
- Law enforcement: Is there a criminal element? If so, has law enforcement been contacted?
- Determine whether the incident triggers notification.
- Insurance: Do you have an insurance that might have to be informed?
- Legal hold: have you applied a legal hold to relevant documents connected with the incident?
- PR and Media: have you developed a communications strategy for this incident?
- Breach remediation provider(s): do you intend to engage breach remediation services?

Download our complimentary Bird & Bird checklist:

Bird & Bird

Build the right incident response team

- Management
- IT
- IT Sec (CSO)
- DPO
- Legal / Compliance
- HR
- Public Relations / Customer Relations

Bird & Bird

Informing data protection authority(ies)

- Notify asap, but not too early
  - Do not use the full 72 hours, unless you must
  - Inform when you have a "presentable" case (i.e. ideally when the breach is already contained, first remediation measures underway)

- How to inform
  - Promise a follow-up notification when all facts are clear
  - Use the follow-up notification to present you in a good light
  - Include as much information about remediation measures as possible

Informing data subjects: make sure to get this right

- When to notify
  - When you have reliable information. If you can, avoid situations where you must correct yourself or send a follow-up notice
  - When you have excluded as many risk factors as possible (e.g. confirmed that no passwords were compromised)
  - Note: The EDPB guidelines require information of data subjects that were *at risk*, even if not actually affected
- How to inform
  - Write the letter as if it could be published (because it might)
  - Use wording that is earnest but calm
  - Explain what the data subjects need to do now (often nothing)
  - In large-scale cases, combine the information with a link to FAQ on the website, which can be updated in case of new information
- In cases that might trigger (mass) damage claims
  - Do not deliver ammunition to mass damage claim organisers (e.g. by admitting negligence)
  - Consider offering the affected persons a voluntary compensation; describe it as "settlement"

How to avoid sanctions?

- Your breach will most likely be handled by a person who is not in charge of imposing fines
- This person would have to take an active decision to hand your case over to the "fine department"

When will the case handler do this?

- If the impression occurs that the breach is a sign of 'system failure' (e.g. to make a profit)
- If the impression occurs that the controller "will not learn it" without a fine
- In cases of high damage or many affected data subjects

Your key messages to the DPA therefore should be:

- This was an accident that could have happened to anyone
- We learned our lesson already (and this is what we learned…)
- The damage is contained (and we already compensated the data subjects by…)

Thank you & Bird & Bird

Gabriel Voisin

Tel. +44 (0) 20 7905 6236

gabriel.voisin@twobirds.com

Dr. Simon Assion

Tel. +49 (0)69 74222 6560

simon.assion@twobirds.com

twobirds.com