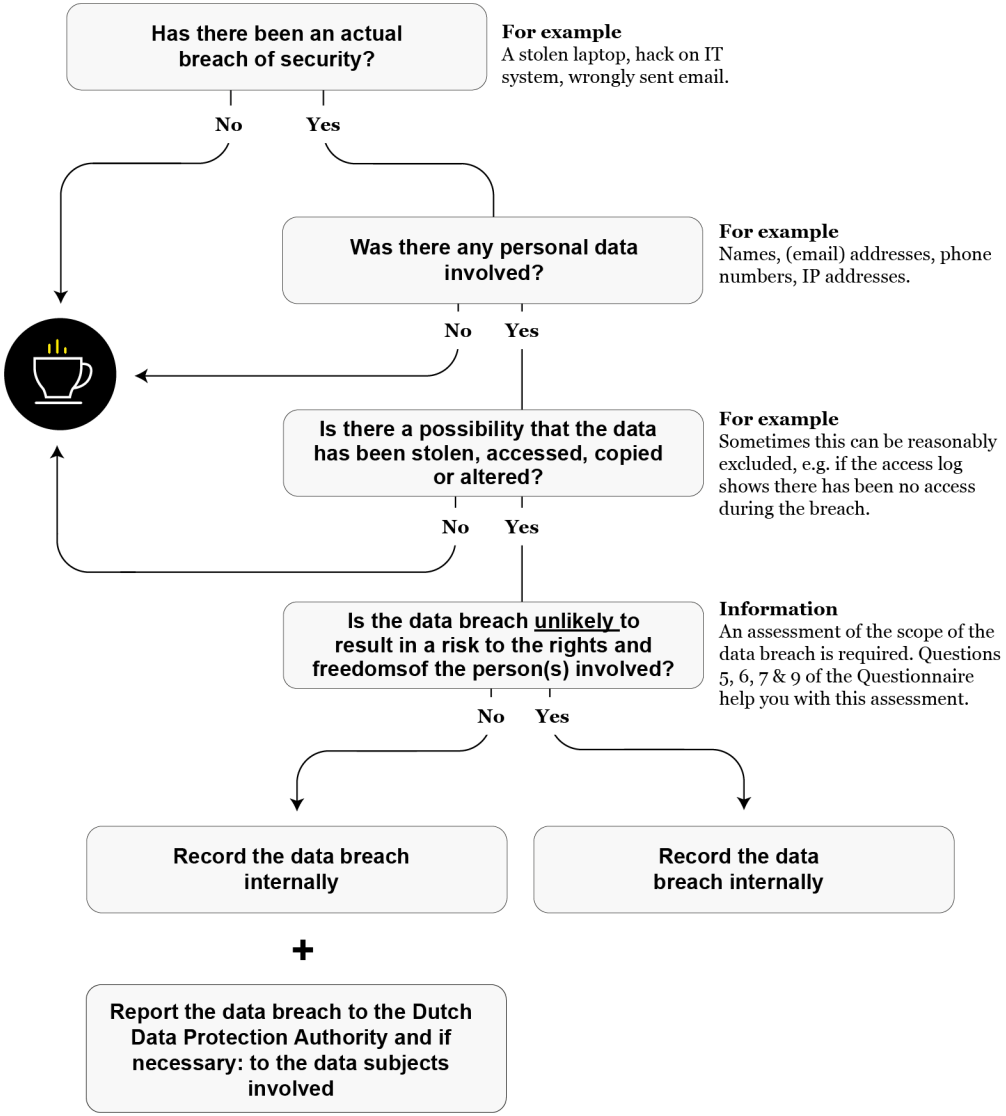
Internal protocol data breaches

LessonUp B.V. (LessonUp)

Table of contents

1. The Protocol in a Nutshell



1. Introduction

Since 2016, the legal obligation to report data breaches applies. This obligation is included and extended in the General Data Protection Regulation (**GDPR**). Organisations must document every data breach. In addition, under circumstances, data breach must also be reported to the supervisory authority – which for LessonUp is the Dutch Data Protection Authority (**DDPA**) (*Autoriteit Persoonsgegevens*) – and communicated to the data subjects involved.

In the event of a (suspected) data breach, it is important to act with due care. The purpose of this protocol is to determine whether there has been a data breach and if so, whether it must be reported.

> ⚠ **It is important to act quickly, because if reporting is necessary, such report must be made within 72 hours after becoming aware of the data breach.**

Therefore, LessonUp (as data controller) should also have in place arrangements with any data processors LessonUp uses, which themselves have an obligation to (immediately) notify LessonUp in the event of a breach.

In order to ensure a fast and efficient data breach process, one or more persons are designated internally to process and handle data breaches. Within LessonUp, this person is:

Tim Meerhof **tim@lessonup.com** **Phone N/A**

Anyone who discovers, becomes aware of or suspects a data breach, shall report this immediately to the person above. This person is responsible for following this protocol properly and to fulfil the obligation the data breach and/or data incident properly.

Please note that the omission to notify a data breach to the DDPA and/or communication to the data subjects may result in sanctions under the GDPR, such as the imposition of the applicable administrative fine[1], either accompanying a corrective measure or on its own. There is no sanction for reporting an incident that ultimately turns out not to be a data breach.

NB: Many privacy specialists advise not to be too reluctant to report a data breach. For example, it may be suspicious if a major company has never made a report to the DDPA. The DDPA also actively investigates data breaches that have not been reported or have been reported too late (see this DDPA message - in Dutch).

> 📞 **Please do not hesitate to contact De Roos Advocaten if you have questions about this protocol, completing the document or handling a data breach.**

2. What to do if a data breach occurs?

This protocol applies to (suspected) data breaches within the organization of LessonUp and to (suspected) data breaches within third-parties that process personal data on behalf of LessonUp (e.g. hosting provider, payment provider or other online tools such as Google, Sendinblue, Dataiku, Pipedrive etc.). For the avoidance of doubt; it concerns data breaches relating to personal data whereby LessonUp acts as data controller.

LessonUp acts as data processor for certain personal data as well. (Suspected) data breaches regarding to those processing activities should be notified to the relevant data controller.

Every data breach, whether or not it has to be reported, and every data incident must be documented internally. **Therefore step 8 of the protocol is always required.** For this purpose, the Questionnaire Data Breaches (attached as **Annex**) shall be completed and retained. You can fill in the Questionnaire Data Breaches with the help of the protocol below.

> ⚠ **Every data incident must be documented internally**

The DDPA may use the (filled in) Questionnaire Data Breaches to check whether a security incident should have been reported or not. More specifically, the (filled in) Questionnaire Data Breaches should enable the DDPA to verify compliance with the obligation concerning the notification and documentation of a data breach as laid down in article 33 of the GDPR.

For organisations that process personal data in different EU Member States and/or process personal data of persons from different Member States, the GDPR has introduced the 'one-stop shop mechanism'. This means that organisations that carry out cross-border processing activities have to deal with just one data protection authority, i.e. the 'lead supervisory authority'.

For LessonUp the lead supervisory authority is the DDPA, since the head office is located in the Netherlands. Therefore, if a data breach must be reported, it should be reported to the DDPA.

[1] Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under article 83(4)(a) GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures.

3. The protocol – a step-by-step

1 Has there been a breach of security?

A data breach consists of a breach of security. There is no breach of security (yet) if there is only a threat of a breach or a failure to secure the personal data adequately. There must have been an actual breach of security.

- Examples of a data breach: stolen laptop with customer data, hack on IT system(s), e-mail containing personal data sent to the wrong person, any unauthorized access (also if this is a result of a third-party data breach) etc.
- Answer questions 3 & 4 of the Questionnaire Data Breaches.
- Has there been a breach of security? *Proceed to step 2.*

2 Is there a personal data breach within the meaning of the GDPR?

An incident is qualified as a 'data breach', if there has been 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.

- Please note: "personal data" is a wide definition and refers to any data that allows a person to be (in)directly identified. Under circumstances, even dynamical IP-addresses qualify as personal data.
- A breach is a type of security incident. However, the GDPR only applies when the breach concerns personal data. The consequence of such a breach is that LessonUp will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. As mentioned before, security incidents, such as receiving a phishing e-mail without opening clickable links/attachments, also need to be reported with the Questionnaire Data Breaches.
- Answer question 5 & 8 of the Questionnaire Data Breaches and *proceed to step 3.*

3 What is the role of LessonUp regarding the personal data involved?

The obligation to document and report a data breach is imposed on the data controller. LessonUp is the data controller of the personal data that are being processed.

- Has there been a data breach involving personal data processed by LessonUp in its role as data controller? If so, *proceed to step 4.*

4 Can unauthorised/unlawful processing of personal data reasonably be excluded?

Sometimes the unauthorised/unlawful processing of personal data may reasonably be excluded, due to the fact technical and organizational measures have been taken. Personal data have been processed unlawfully e.g. if they were stolen, if an unauthorized person has accessed, copied or altered them or if the personal data have been deleted or destructed if this was not intended.

- Determine whether the unauthorised/unlawful processing of the personal data may be excluded, by technical and organizational measures. For example, if the log files show there was no access to any personal data by an unauthorized person.
- In the event the unauthorised/unlawful processing of personal data can reasonably be excluded, there is no data breach.
- In the event the unauthorised/unlawful processing of personal data cannot reasonably be excluded, there is a data breach. *Proceed to step 5.*

5 Determine the scope (and risks) of the data breach.

- Answer questions 5, 6, 7 & 9 of the Questionnaire Data Breaches and *proceed to step 6.*
- When assessing the risk to individuals as a result of a breach, LessonUp should consider the specific circumstances of the breach, including the

severity of the potential impact and the likelihood of this occurring. It is recommended to take into account the following criteria with the assessment: i) the type of breach, ii) the nature, sensitivity, and volume of personal data, iii) ease of identification of individuals, iv) severity of consequences for individuals,
v) special characteristics of the individual, vi) special characteristics of the data controller, vii) the number of affected individuals, viii) any other relevant circumstances.

6 Notification to the DDPA.

A data breach must be reported to the DDPA, unless the data breach is unlikely to result in a risk to the rights and freedoms (e.g. privacy) of natural persons (the data subjects).

- Based on the information available and set out under step 5, determine whether the data breach might result in a risk to the rights and freedoms (e.g. privacy) of natural persons.
- If the data breach does result in a risk as described above, report the data breach to the DDPA via the online reporting form (NB: in Dutch). In addition, *proceed to step 7*.
- If the data breach does not result in a risk as described above, the data breach does not have to be reported to the DDPA, *skip step 7 and proceed to step 8*.

7 Communication to the data subjects.

If the data breach is likely to result in a high risk to the rights and freedoms (e.g. privacy) of natural persons, the data breach must also be communicated to the data subjects. The DDPA may also order organizations to report a data breach to the data subjects.

- Determine whether the data breach is likely to result in a high risk to the rights and freedoms (e.g. privacy) of natural persons. When in doubt, contact De Roos Advocaten (or the DDPA) to check whether the data breach must be communicated to the data subjects.
- If the data breach must be communicated to the data subjects, such communication must at least contain the following information (in clear and plain language):
  - A description of the **nature of the personal data breach**;
  - The **name** and **contact details** of the data protection officer or other contact point within LessonUp where more information can be obtained;
  - A description of the **likely consequences** of the personal data breach;
  - A description of **the measures taken or proposed** to be taken by LessonUp to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

  NB: The criteria for communicating to the data subjects are higher than those for reporting to the supervisory authority. Therefore, a data breach can never only be communicated to the data subjects – in such cases the data breach must also be reported to the DDPA.
- Retain a copy of the notification to the data subjects.
- *Proceed to step 8.*

8 Internal documentation obligation.

Every data incident and/or data breach must be recorded internally, even if the data breach does not have to be reported to the DDPA / data subjects.

- Answer the remaining questions in the Questionnaire Data Breaches.
- Retain a copy of the filled in Questionnaire Data Breaches (in PDF) within the systems of LessonUp.

Annex: Questionnaire Data Breaches

Please note that this Questionnaire is for internal use and is therefore in English. However, if the data breach must be reported with the DDPA, the report must be filed in Dutch via the report form on the DDPA website.

1	**When was the data breach discovered?**	[DD/MM/YYY] at [time]
2	**Describe the date and time of the data breach.** *This can be a specific time or a period. If not clear, please fill in 'unknown'.*	[DD/MM/YYY] at [time] / [PERIOD]
3	**Describe the data breach (as detailed as possible)** *Please describe what took place, where and if possible, the cause. Examples of a data breach: stolen laptop with customer data, hack on IT system(s), e-mail containing personal data sent to the wrong person, any unauthorized access (also if this is a result of a third-party data breach) etc.*	[description]
4	**Wat is the nature of the data breach?** *Answer per category and complete where necessary.*	○ An unauthorized person can access the personal data: YES / NO ○ The personal data are or can be copied by an unauthorized person: YES / NO ○ The personal data/source data are or can be altered (e.g. a hack in the system): YES / NO ○ The personal data/source data are or can be deleted or destroyed (e.g. ransomware or fire in the data center): YES / NO ○ Personal data were stolen: YES / NO ○ Other: [description]
5	**Describe the categories of data subjects affected by the data breach (who's personal data were leaked?).** *For example: clients, employees, customers, etc.*	[description]
6	**The personal data of how many people were affected by the data breach?** *Specify a minimum and maximum number.*	[number] – [number] persons

7	**Is one of the specific categories of persons affected?**	Elderly: YES / NO Children/minors: YES / NO Sick or mentally/physically disabled: YES / NO
8	**Which (categories of) personal data are involved in the data breach?** *For example: name, address, phone number, e-mail address, login details, financial details, social security number, gender, profile picture, biometrical data, school or work performance, medical data, relationship details, religion, political beliefs, sexual preferences, etc.*	[description]
9	**What are the possible effects/consequences of the data breach for the data subjects involved?** *For example: risk of stigmatization or exclusion, risk of identity fraud, risk of financial damage, risk of reputational damage, risk of exposure to spam or phishing, etc.*	[description]
10	**What remedial action (by e.g. (prior) technical and organisational measures) have been taken to stop the data breach and to prevent further data breaches?** *If necessary, consult this section with your IT-department.*	[description]
11	**Are the personal data involved being processed / leaked outside EER?**	YES/NO If so: [description of the countries to which the data have leaked]
12	**Please document the reasoning for the decisions taken in response to a breach.** *In particular, if a breach is not reported to the DDPA/data subjects, a justification for that decision should be documented. This should include reasons why LessonUp considers the breach is unlikely to result in a (high) risk to the rights and freedoms of individuals.* *When assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify.*	[description]
13	**Other relevant information regarding the data breach.**	[description]