Data leak Protocol

1. ***Introduction***

This document describes the various steps which should (must) be taken within Lead Leaders B.V. in the event of a data leak, within the meaning of Article 4, paragraph 12 of the General Data Protection Regulation (GDPR).

Under 'management' should be understood; Mrs. Linda van Liempt

2. ***Responsibilities***

Official	**Responsibilities**
Executive Board	Adopting and registering reports of data leaks
Executive Board	Report a data leak to the Dutch Data Protection Authority, **if necessary.**
Executive Board	Assessing and recording consequences and measures to be taken
Executive Board	Approval of measures
Employees	Reporting data leaks of personal data

3. ***Description of Procedure***

The obligation to report data leaks originates from the GDPR. In the event of a data leak, there is a breach of the security of personal data (as referred to in Article 4, paragraph 12 GDPR). The personal data is then exposed to loss or unlawful processing.

Data leaks could arise from:

- willful acts (cyber-crime, hacking, identity fraud, malware contamination);
- technical failure (ICT failures);
- human failure (too simple passwords/providing user name/password to colleagues and external parties);
- unlawful processing of data;
- lost USB stick or laptop;
- sending emails with email addresses of all recipients;

3.1 Report to the Dutch Data Protection Authority and the parties involved

3.1.1 *Dutch Data Protection Authority*

A data leak must be reported immediately (within 48 hours) after Lead Leaders B.V. has learned of it, to the Dutch Data Protection Authority.

The data leak must also be reported to the involved parties when it is likely that the leak will result in a high risk to its rights and freedoms, in order to be able to take precautionary measures.

The involved parties are those whose personal data are involved in a leak. In the event of Lead Leaders B.V. this is usually individuals who have agreed to receive messages from Lead Leaders B.V, (possibly) its clients and/or its employees. The involved parties have to be informed immediately of the leak if the infringement is likely to have adverse consequences for his/her privacy.

A report to the parties involved may be omitted if measures were taken afterwards by the controller to ensure that there will likely be no further privacy risks, or the report requires disproportionate effort.

3.2 Step-by-step plan for internal reporting

3.2.1 *Step 1: Reporting a data leak*

All data leaks of personal data must be reported to management. The report can be made by any employee and any processor. The report can also be made by an external person to an employee of Lead Leaders B.V. The report must be made directly and per telephone to management, and recorded in writing by the reporter. Management can also be contacted outside of office hours to report a data leak.

Management records:

- the name of the reporter;

- date and time of the report;
- nature of the infringement (is there significant risk of loss or unlawful processing?);
- which personal data does the report relate to;
- what amount and/or data records are involved;
- which (groups) persons are involved in the report;
- which measures are or will be taken by the reporter;
- what are the consequences, for the involved parties, according to the reporter;
- the contact person for the report.

3.2.2 *Step 2: Inventory of consequences and measures to be taken*

After receiving a report of a data leak, the management of Lead Leaders B.V. reviews and records:

- the necessary follow-up actions with regard to the data leak (immediately closing the leak, restricting access to information and at the same time gathering more information about the intruder;
- which will be reported to the Dutch Data Protection Authority by the management of Lead Leaders B.V. (in addition to nature of the infringement, which personal data, number of persons/records involved):
- the possible consequences for the involved parties;
- the measures that Lead Leaders B.V. take and/or can take to reduce the damage for the involved parties;
- the measures that can be taken by those involved to reduce further damage, including the manner of informing about this;
- contact details for involved parties;
- the manner of internal handling, including communication to reporter, involved department(s) and team leader(s);
- whether personal or third party liability is involved, such as due to breach of contract (because an obligation of confidentiality has been violated, or inadequate security has been realized in violation of a contractual obligation) or due to an unlawful act;
- whether or not to file a report and to determine whether criminal liability is involved. This can for example be when there is involvement from Lead Leaders B.V. itself, a processor, or when insufficient measures have been taken to prevent irregularities. Consultations with the legal adviser are possible, if required;
- what is communicated internally, at what time; what is externally communicated, at what time.
- what is communicated externally, at what time? It is determined whether the press should be informed;
- or other stakeholders must be informed in addition to the Dutch Data Protection Authority;
- the manner in which an internal report is reported, including the action holder;
- whether possible damages are covered by the insurance policy.

Possible improvement/management measures are recorded in the *Improvement Register*.

3.2.3 *Step 3: Approval*

The director approves the activities to be performed, as determined, or amends the activities to be carried out. The activities determined by the director are carried out.

3.2.4 *Step 4: Reporting to the Dutch Data Protection Authority*

The management will report the data leak to the Dutch Data Protection Authority, at the latest, within 2 days. In any case, the following will have to be reported:

- nature of the infringement, including the categories involved, the number of parties involved, number of data records;
- description of the consequences to be expected;
- measures taken and/or proposed;
- information on measures to be taken by the involved parties to limit the adverse consequences;
- contact details for the involved parties.

3.2.5 *Step 5: confirmation of receipt of the Dutch Data Protection Authority*

If a report was made then Lead Leaders B.V. will receive a confirmation of receipt. With reports that give rise to further action by the Dutch Data Protection Authority, the Dutch Data Protection Authority will contact Peter Ruiter to verify the origin of the report.

3.3 Absence of management

In the absence of management, this role will be filled by Ivonne Keijzers.