

Le Bélier Magyarország Formaöntöde Zrt.

Data Protection Policy

___ October 2018

Issued by: name, position

.....

Contents

1	GENERAL PROVISIONS	4
1.1	INTRODUCTORY PROVISIONS	4
1.2	REVIEW DATE	4
1.3	THE SCOPE OF THE POLICY	4
1.4	REFERENCES	4
1.5	REVISION HISTORY	5
1.6	DEFINITIONS	5
1.7	THE OBJECTIVE OF THE DATA PROTECTION POLICY	6
2	DATA PROCESSING AND DATA HANDLING	7
2.1	DATA PROCESSING AT LE BÉLIER MAGYARORSZÁG FORMAÖNTÖDE ZRT.:	7
2.2	OUTSOURCING AT LE BÉLIER MAGYARORSZÁG FORMAÖNTÖDE ZRT.	8
3	RESPONSIBILITY	9
3.1	PERSONAL RESPONSIBILITY	9
3.2	THE RESPONSIBILITY OF LE BÉLIER MAGYARORSZÁG FORMAÖNTÖDE ZRT., POSSIBLE CONSEQUENCES OF UNLAWFUL DATA PROCESSING	9
4	THE PERSON RESPONSIBLE FOR DATA PROTECTION	10
5	ENSURE THE LAWFULNESS OF DATA PROCESSING	12
5.1	DATA PROTECTION IMPACT ASSESSMENT	12
5.1.1	<i>Mandatory cases</i>	12
5.1.2	<i>The content of data protection impact assessment</i>	12
5.1.3	<i>Preliminary consultation</i>	13
5.2	EXERCISE OF DATA SUBJECT RIGHTS	13
5.2.1	<i>The requirement of providing prior notice</i>	13
5.2.2	<i>Notification, objection, correction, erasure (blocking, restriction), complaint</i>	14
5.3	DATA TRANSFER AND DISCLOSURE	15
5.4	CONTRACTS AFFECTING PERSONAL DATA	16
6	DATA SECURITY	19
6.1	GENERAL DESCRIPTION OF DATA SECURITY MEASURES	19
6.2	MANAGEMENT OF A DATA BREACH	19
6.2.1	<i>Investigation of a data breach, and notification of the Authority</i>	19
6.2.2	<i>Communication of a personal data breach to the data subject</i>	20
6.2.3	<i>Records</i>	21
7	DATA PROCESSING AT THE WORKPLACE - SPECIAL RULES	22
8	OTHER PROVISIONS	23
8.1	DATA QUALITY	23
8.2	RECORDS OF CONTROLLERS AND PROCESSORS	23
8.3	ERASURE	23
8.4	LIAISON WITH THE AUTHORITY	23
8.5	TRAINING	24
	ANNEX 1: RECORDS OF PROCESSING ACTIVITIES	25
	ANNEX 2: BALANCING TEST (TEMPLATE)	26
	ANNEX 3: DATA PROTECTION IMPACT ASSESSMENT (TEMPLATE)	28

ANNEX 4: DATA BREACH REGISTER	30
ANNEX 5: EMPLOYEE DATA PRIVACY NOTICE.....	31

1 General Provisions

1.1 Introductory provisions

The objective of this Regulation is to identify the detailed rules of the management, protection and security of the personal data managed and processed by Le Bélier Magyarország Formaöntöde Zrt. (name of appropriate entity to be inserted), and to comply with the requirement of accountability.

1.2 Review date

The Person responsible for data protection shall arrange the review of this Regulation in the following cases:

- regularly every year,
- before 31 December of each year,
- if the legal provisions and regulatory documents identified in 1.4 are materially changed.

1.3 The scope of the Policy

- Personal scope: it shall apply to all organisational entities of Le Bélier Magyarország Formaöntöde Zrt., all natural persons working therein, particularly, but not exclusively to employees, sub-contractors and suppliers.
- Substantive scope: it shall apply to all activities of Le Bélier Magyarország Formaöntöde Zrt. performed on personal data, including data management, data processing and data security, as well as the related rights and obligations.
- Time scale: The Policy shall be valid from its taking effect until repelled or, until the next version of the Policy takes effect.
- The Policy shall be applied jointly with the related legal provisions and policies referred to in 1.4.

1.4 References

Related policies:

- *List here all policies at the entity that are relevant from a data protection (e.g. Company policy, IT Security Policy, Remote Work Policy)*

Relevant legal provisions:

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (“Information Act”)

-
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”)
 - Act I of 2012 on the Labour Code (“Labour Code”)
 - Act CXXXIII of 2005 on the rules of personal and property protection activities and private investigation (“Security Services Act”)

1.5 Revision history

Version number of this Policy: v 1.1 (Approval date: __)

Version number of previous Policy:

1.6 Definitions

Data handling (technical data processing): performance of technical tasks related to data processing operations irrespective of the methodology and device used for performing the operations, or of the site of application provided technical tasks are performed on data.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data transfer: Making data available to a specific third party.

Data subject: A natural person that has been or can be identified by some information.

EEA state: member states of the European Union, other states party to the Agreement on the European Economic Area (EEA), further, a state whose citizens enjoy the same rights as those of a state party to the Agreement on the EEA subject to an international treaty concluded between the European Union and its members states and a state not party to the Agreement on the EEA.

Third country: any country that is not an EEA state.

Authority: the supervisory authority for the protection of personal data, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH).

Consent: a freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal data: any information relating to an identified or identifiable natural person ("data subject").

1.7 The objective of the Data Protection Policy

The objective of the Data Protection Policy is to ensure that Le Bélier Magyarország Formaöntöde Zrt. protects personal data through an internal policy in compliance with Hungarian and European legal provisions including particularly the constitutional principles of data protection, the right to informational self-determination and the requirements of data security.

Le Bélier Magyarország Formaöntöde Zrt. is committed to observe the legal provisions relating to personal data. Therefore, the Data Protection Policy shall identify the major tasks and the related competences with reference to the protection of personal data at Le Bélier Magyarország Formaöntöde Zrt.

The Policy shall constitute the data protection and data security framework of Le Bélier Magyarország Formaöntöde Zrt. together with the policies referred to in 1.4.

2 Data processing and data handling

2.1 Data processing at Le Bélier Magyarország Formaöntöde Zrt.:

Le Bélier Magyarország Formaöntöde Zrt. can process personal data if it has a lawful purpose related to data processing (purpose limitation) and the proper legal basis.

In addition to the properly concrete and accurate identification of the lawful purpose of data processing, the legal basis of the data processing must also be identified from among the following:

- Legal obligation;
- Consent of the data subject;
- Legitimate interest of Le Bélier Magyarország Formaöntöde Zrt.;
- Contractual obligation;
- Vital interest;
- Public interest.

In the course of data processing Le Bélier Magyarország Formaöntöde Zrt. shall comply with the following principal requirements:

- Privacy by design;
- Principle of fairness;
- Principle of accuracy;
- Requirement of prior notification;
- Respect of the rights of data subjects, particularly the right to information and legal remedy and the right to erasure;
- Principle of data minimisation and storage limitation;
- Prevention and management of personal data breaches.

The details of Le Bélier Magyarország Formaöntöde Zrt.'s data processing activities are included and updated regularly by the person responsible for data protection in the records of processing activities attached as Annex 1.

Le Bélier Magyarország Formaöntöde Zrt. only processes special categories of personal data ("sensitive data") in limited cases: employee data (possibly data of employees' relatives) related to absence due to sickness or data related to the medical fitness of employees or potentially employee data related to membership in interest representation bodies. Processing of criminal personal data takes place in response to claims by the investigating authority. If special or criminal personal data

are processed, increased attention must be paid to the specific legal provisions regulating processing of such data.

2.2 Outsourcing at Le Bélier Magyarország Formaöntöde Zrt.

Certain activities which involve personal data are outsourced by Le Bélier Magyarország Formaöntöde Zrt. to other members of the Le Bélier Group or to third party service providers.

These activities are the following (to be listed here, including contracts through the parent company, e.g. SAP):

- Physical security: Det-Őr Kft.

-

3 Responsibility

3.1 Personal responsibility

All persons subject to this Policy are responsible for properly executing the provisions of the Policy and are obliged to immediately report any violation of data protection related rules to their line manager or directly to the person responsible for data protection.

The head of the organisational unit involved in data processing is responsible for ensuring that the handling and processing of personal data comply with the relevant legal provisions and with this Policy.

The head of the organisational unit involved in data processing is responsible for ensuring that the organisational unit only processes and handles personal data in accordance with the objectives and legal basis of data processing, no out of scope data processing or handling shall be made, no material decision shall be made affecting data processing or data handling.

The head of the organisational unit shall immediately initiate discussions with the person responsible for data protection if they learn (or suspect) about the violation of the rules related to personal data or if they or their subordinates have questions with respect to the processing and handling of personal data.

The violation of the provisions of this Policy is a serious breach of rules, and may result in disciplinary action.

3.2 The responsibility of Le Bélier Magyarország Formaöntöde Zrt., possible consequences of unlawful data processing

Le Bélier Magyarország Formaöntöde Zrt. is responsible for compliance with data protection regulations. The Authority may impose a fine up to 4% of the Le Bélier Group's annual turnover in the case of a serious breach of data protection regulations.

In addition, a data subject has the right to enforce a claim against Le Bélier Magyarország Formaöntöde Zrt. under civil law in the form of objective based grievance fee or compensation.

Personal data are also protected by criminal law (criminal offence of misuse of personal data).

4 Designated person responsible for data protection

In order to protect personal data and enforce the rights of data subjects, Le Bélier Magyarország Formaöntöde Zrt. has designated a person responsible for data protection (local person to be determined) to provide local support to the Group Data Protection Officer (Benoit Millet; Phone: +33(0)5 57 55 03 55; Mobile: +33(0)7 61 23 19 65; E-mail: benoit.millet@lebelier.fr). The person responsible for data protection acts independently within his/her competence, and may not be given orders. The person responsible for data protection must be involved in making a decision on any issue affecting personal data or in the preparation of such decisions already when an issue arises or in the early phase of the preparation of a decision.

The contact details of the person responsible for data protection _____ (name, position) is as follows:

- E-mail address:
- Telephone number:

All persons subject to this Policy shall collaborate with the person responsible for data protection and provide him or her with the information, resources and authentications that are necessary for performing his or her tasks.

Within its competence, and in accordance with the relevant legal provisions, the person responsible for data protection shall with the involvement of the Group Data Protection Officer and – if necessary – the affected business areas or third party legal representation:

- Provide information and advice related to the protection of personal data, monitor and control compliance with the legal provisions and internal policies relating to personal data.
- Monitor the changes of data protection rules and practice (with particular attention to the documents issued by WP29 Working Team and the Authority), if necessary making recommendations for the amendment of policies and processes.
- Promote the exercise of the rights of data subjects; investigate complaints affecting personal data and initiate measures to remedy such complaints.
- Liaise with the Authority.
- Coordinate and manage data protection impact assessments. Coordinate the amendment of this Policy and data processing notice and contribute to the modification and upgrading of policies and training materials relating to data protection.
- Keep records of data processing and data handling that of the incidents of data protection and the records of data transfer, and ensure that data protection training sessions are delivered.

-
- In the event of data processing based on legitimate interest, he/she shall coordinate the balancing test (Annex 2).

5 Ensure the lawfulness of data processing

Le Bélier Magyarország Formaöntöde Zrt. shall take the following measures to ensure compliance with the legal provisions relating to personal data:

5.1 Data protection impact assessment

If, taking into account its nature, scope, circumstances and purpose, data processing is assumed to involve high risk regarding data subjects' rights, then – prior to its commencement – Le Bélier Magyarország Formaöntöde Zrt. shall carry out an impact assessment to ascertain how the planned data processing activities affect the protection and security of personal data. Data processing activities that are similar in nature and carry similar risks can be assessed within the same impact assessment.

The person responsible for data protection shall coordinate the execution of the impact assessment. Processing activities may not be introduced or modified without approval by the person responsible for data protection.

5.1.1 Mandatory cases

A data protection impact assessment shall be performed particularly in the following cases:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- Processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences;
- The systematic monitoring of a publicly accessible area on a large scale.

Primarily, the head of the organisational unit in whose competence a given data processing activity arises shall decide on the necessity of data protection impact assessment by answering the questions in Annex 3. If data protection impact assessment is deemed necessary, the head of the organisational unit shall inform the person responsible for data protection who will coordinate the impact assessment as described in 5.1.2.

5.1.2 The content of data protection impact assessment

The minimum content of a data protection impact assessment is the following:

- A systematic description of the planned data processing operations identifying the purpose and legal basis of data processing including, if relevant, the legitimate business interest of the controller.

-
- Assessment of the necessity and proportionality of data processing operations with respect to the purposes of data processing;
 - Assessment of the risks affecting the rights and freedoms of data subjects; and
 - The description of the measures aimed to manage risks including the guarantees and security measures and mechanisms to protect personal data and compliance with the legal requirements taking into account the rights and legitimate interests of the data subjects and other persons.

Le Bélier Magyarország Formaöntöde Zrt. regards data protection impact assessment as a dynamic process rather than a static snapshot; therefore the person responsible for data protection must monitor and check data processing operations and assess if the processing of personal data complies with the data protection impact assessment. A new impact assessment must be performed if the risks related to data processing have changed.

5.1.3 Preliminary consultation

If the impact assessment establishes that data processing likely carries high risk due to the lack of risk mitigating measures, the person responsible for data protection must inform the head of the organisational unit in the scope of activities of which the necessity of data processing has risen. Then consultations must be made on alternative solutions to mitigate the risk.

If using alternative solutions, the risk cannot be mitigated to an extent acceptable to the person responsible for data protection and the data processing still seems to be necessary, Le Bélier Magyarország Formaöntöde Zrt. must consult with the Authority prior to commencing the data processing activity.

In the course of the consultations the person responsible for data protection shall inform the Authority:

- Of the roles and responsibilities of the controller, joint controllers and processors involved in the data processing,
- On the purposes and method of the planned data processing;
- On the measures taken and guarantees provided to protect the rights and freedoms of data subjects;
- On the availability of the person responsible for data protection;
- On the data protection impact assessment; and
- Any other information requested by the Authority.

After the consultations actions must be taken subject to the recommendations of the Authority.

5.2 Exercise of data subject rights

5.2.1 The requirement of providing prior notice

Le Bélier Magyarország Formaöntöde Zrt. processes personal data so that they are also transparent for the data subjects. Therefore, it publishes a detailed and easy to understand privacy notice on its website with minimum the following content:

- Name of controller;
- Purpose of data processing;
- Legal basis of data processing;
- Scope of data controlled;
- Scope of data processed;
- Time period of data processing;
- Information about data processors;
- Persons authorised to access the data;
- Information about data security measures (properly detailed for the data subjects but in such a way that the detailed nature of the information cannot be a threat to data security);
- Data processing based on legitimate interest;
- Data subject rights and legal remedies.

The person responsible for data protection shall monitor if the privacy notice is updated, and update it immediately if necessary, but at least once a year.

5.2.2 Notification, objection, correction, erasure (blocking, restriction), complaint

Data subjects have the right to request information regarding the processing of their personal data via the options indicated in the data processing notice of Le Bélier Magyarország Formaöntöde Zrt. Further, data subjects have the right to object to processing their personal data or to ask for their correction or erasure (blocking, restriction) in specific cases. Data subjects may, in addition, lodge a complaint at any time, if they have suffered (real or assumed) damage with respect to their personal data. Le Bélier Magyarország Formaöntöde Zrt. shall take all reasonably expected measures to ensure that data subject questions (requests) are managed properly.

The person responsible for data protection shall coordinate replies given to the request for information, correction or erasure and the investigation of complaints as follows:

- The person responsible for data protection shall forward the document containing the question (request) received from a data subject to the head of the organisational unit involved in the given data processing (if several organisational entities may be involved, the documents shall be forwarded to all of them). If the question (request) by a data subject was not received by the person responsible for data protection, it shall be immediately forwarded to the person responsible for data protection.

-
- Every case shall be reviewed and replied to individually by reviewing the regulations (particularly the Information Act and GDPR) and their interpretation. If the question (request) cannot be unambiguously judged, the legal entity must be involved in the reply.
 - The head of the organisational unit performing the processing activity is responsible for providing the person responsible for data protection with the necessary and accurate information to respond to the question (request), so that an easy-to-understand written response can be provided within the shortest time after receipt but no later than **within 15 days**.
 - The response to data subject questions (requests) shall be justified and approved by the person responsible for data protection. In the reply the data subjects shall be informed about the options of legal remedy in every case. In the course of information on legal remedy, the availability of the Authority and the court must be provided in every case, and data subjects are to be advised to turn to Le Bélier Magyarország Formaöntöde Zrt. if they have any further questions.
 - If the case requires further measures to be taken by Le Bélier Magyarország Formaöntöde Zrt. (e.g. erasure, blocking or restriction), the measures shall be executed and documented in collaboration with the person responsible for data protection without delay.

If a question (request) by a data subject may also be considered to be a complaint, the grounds for the (justified) complaint must be generally eliminated. The entities taking part in complaint management must pay particular attention to the proper resolution of complaints made repeatedly and the related communication.

If a question (request) by a data subject also involves information Section 5.3 refers to (e.g. request to be informed if certain data have been forwarded to some authority) the person responsible for data protection shall involve the legal entity before replying and must review using special care whether the requested information may be issued to the data subject in compliance with relevant law.

5.3 Data transfer and disclosure

The person responsible for data protection shall be informed if Le Bélier Magyarország Formaöntöde Zrt. receives a claim for data transfer or disclosure affecting personal data (typically by an authority or court).

The identification of the legal basis and the purpose of a claim received must be checked individually in every case. If the legal basis and the purpose are not identified, the requesting entity shall be called for clarification. If the legal basis and purpose are identified, their lawfulness must be checked before data transfer or disclosure and the requesting entity shall be called for clarification if necessary. If a claim cannot be unambiguously judged, the legal entity must be involved in the reply (and in identifying its scope). A claim for data transfer or disclosure cannot be fulfilled if it is not lawful (and/or its purpose is not or not fully clarified or if its legal basis is unclear).

The head of the organisational unit in whose competence the claim has arisen shall be responsible for preparing data transfer or disclosure. No data can be transferred or disclosed lacking the approval of the person responsible for data protection. In the event of replying to a high number of claims with the same legal basis and purpose (e.g. claims by police authorities) the above procedure may be disregarded with permission by the person responsible for data protection. The person responsible for data protection shall keep records of the data transferred.

In the event of data transfer within the Le Bélier Group the lawfulness of the planned data transfer must also be checked. If the question cannot be unambiguously judged, the person responsible for data protection must be involved in the decision.

Data transfer may be directed to EEA countries or to third countries. Data transfer to EEA countries shall be regarded as if the data transfer took place within the territory of Hungary.

Le Bélier Magyarország Formaöntöde Zrt. may transfer personal data to a controller involved in data processing in a third country or it can transfer personal data to a processor performing data handling in a third country if the data processing is inherently lawful, and the Data Subject has consented to the transfer in writing or it is based on legal authorisation or provision provided that the rights of the third country in question grant proper protection - as identified by the European Union - for the processing and handling of the data transferred, further, the criteria of data processing are met with respect to all data by the foreign controller.

5.4 Contracts affecting personal data

Le Bélier Magyarország Formaöntöde Zrt. may involve certain Le Bélier affiliates or third party service providers in activities affecting personal data subject to the relevant contracts.

In such an event, the head of the organisational unit preparing the contract shall ensure that the person responsible for data protection is involved in the initial phase of drafting. The comments of the person responsible for data protection regarding the contract must be taken into consideration.

In the course of concluding contracts affecting personal data the following requirements related to the protection and security of personal data must be included:

- The party entering into an agreement with Le Bélier Magyarország Formaöntöde Zrt. shall make a statement that it is aware of the Hungarian and European legal provisions and best practices relating to personal data protection, as well as the internal policies of Le Bélier Magyarország Formaöntöde Zrt., and will act accordingly. The contracting party must be made aware of the policies relating to the subject of the contract at least in a summary form.
- It must be included in the contract whether the party entering into contract with Le Bélier Magyarország Formaöntöde Zrt. acts as a processor (subject to the instructions of Le Bélier Magyarország Formaöntöde Zrt.) or a (co)controller.

-
- The subject of data handling and data processing, the data processing tasks to be performed, their time scale and (potentially automated) nature and purpose must be identified in the contract with respect to personal data.
 - It must be included in the contract that the contracting party shall take all technical and organisational measures to protect personal data from unauthorised access and unlawful use, further, it shall protect them from data loss, damage or change, and that persons should only have access to personal data if they have the proper authorisation and only in order to execute this Contract.
 - The technical and organisational measures taken by the contracting party in order to guarantee a high level of data security relevant to the extent of the risk must be detailed in the contract.
 - It must be included in the contract that the contracting party shall immediately inform Le Bélier Magyarország Formaöntöde Zrt. in the event of any damage to the security of the data (data breach) or a direct or indirect threat thereof.
 - It must be included in the contract that the contracting party only handles or processes personal data subject to the terms and conditions of the contract and may not transfer them to others lacking a special permission.
 - It must be included in the contract that every person with access to the data must be properly informed and trained with respect to processing personal data and must be aware of the confidential nature of the data and of their own obligation of confidentiality. The training must be documented.
 - It must be included in the contract that the contracting party may only involve another processor having the preliminary written consent by Le Bélier Magyarország Formaöntöde Zrt. and only if the other processor shall ensure the protection and security of the personal data to the extent equal to that of the contracting party.
 - It must be included in the contract that the contracting party shall irrevocably erase all personal data after the completion of service provision or shall return them to Le Bélier Magyarország Formaöntöde Zrt. and erase all relevant copies.
 - It must be included in the contract that the contracting party makes available any information to Le Bélier Magyarország Formaöntöde Zrt. that is necessary to verify fulfilment of the obligations identified in the contract, in addition, that allows and supports any audit including on-site inspections performed by the Customer or an auditor appointed by it or by an authority.
 - It must be recorded in the contract that the contracting party acknowledges that violation of its contractual or legal obligations related to personal data shall be deemed a grave breach of contract and may result in immediate termination of thereof.

Deviation from the above is only possible after the related risks have been assessed, with consent by the person responsible for data protection and the legal entity in a documented way.

Special attention must be paid to upgrading the data processing information of Le Bélier Magyarország Formaöntöde Zrt. whenever a contract affecting personal data is concluded.

6 Data security

The data security framework at Le Bélier Magyarország Formaöntöde Zrt. is provided by the totality of the provisions of the policies referred to in 1.4, so all regulations referred to in 1.4 shall be interpreted and applied jointly when dealing with data security issues.

6.1 General description of data security measures

Le Bélier Magyarország Formaöntöde Zrt. provides technical and organisational measures to secure the electronic or paper-based personal data processed or handled by it, i.e. no damage to data security could occur resulting in accidental or unlawful destruction, loss, change, unauthorised publication or unauthorised access to the personal data transferred, stored or processed in any other way (data breach).

If, despite the above, a data breach occurs, Le Bélier Magyarország Formaöntöde Zrt. shall act subject to the provisions of 6.2. with regard to investigating the incident, the involvement of the person responsible for data protection, notification of the data subjects and the Authority and the documentation of the breach and their immediate management.

Every operation relating to personal data is electronically logged in the systems of Le Bélier Magyarország Formaöntöde Zrt. Logged data can only be disclosed in the cases identified in legal provisions, subject to approval by the person responsible for data protection.

6.2 Management of a data breach

6.2.1 Investigation of a data breach, and notification of the Authority

All employees of Le Bélier Magyarország Formaöntöde Zrt. are obliged to report if they perceive or suspect a data breach. The relevant report shall immediately be made to the person responsible for data protection. The following shall particularly (but not exclusively) be deemed data breaches: hacker attacks, theft of data, accidental data leakage, and loss of paper-based documents or data sticks, etc.

The person responsible for data protection shall immediately investigate the data breach (its suspicion) involving the employees affected by the incident and document the findings of the investigation in writing. The investigation documents must include at least the following information.

- What happened?
- Where did it happen?
- When did it happen?
- What personal data are (might be) affected?

-
- (Approximate) number of data subjects.
 - Measures taken to resolve the incident (if any).
 - Other circumstances, consequences and information that are material to the incident.

If Le Bélier Magyarország Formaöntöde Zrt. is deemed the controller of the data affected, the person responsible for data protection shall report the data breach on the electronic interface provided by NAIH within 72 hours except if the data breach is assumed not to carry any risks regarding the rights and freedoms of natural persons. The exception rule can be applied on the basis of the investigation documents with written approval by the leading officer and the person responsible for data protection.

In the report to NAIH:

- The nature of the data breach must be described including if possible, the group and the approximate number of data subjects affected as well as the group and approximate volume of data affected by the incident;
- The name and availability of the person responsible for data protection or another contact person appointed to provide further information must be given.
- The probable consequences resulting from the data breach must be described;
- The measures taken or planned by the controller to mitigate any adverse consequences resulting from the data breach as well as other measures must be described.

If all the above information cannot be provided at the same time, it can be provided in parts later on.

In the event of cross-border data processing, if a data breach affected data transferred to Le Bélier Magyarország Formaöntöde Zrt. by the controller of another EEA country or data transferred to the controller of another EEA country by Le Bélier Magyarország Formaöntöde Zrt., the person responsible for data protection shall immediately inform the controller of the relevant EEA country of the above.

If the report fails to be made within 72 hours, the reasons justifying the delay must also be attached.

6.2.2 Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the person responsible for data protection shall communicate the personal data breach to the data subject without undue delay.

The communication shall include:

- The nature of the data breach described clearly and in an easy-to-understand way;
- The name and availability of the person responsible for data protection or other contact person providing further information;
- The probable consequences resulting from the data breach;

-
- The measures taken or planned to resolve the data breach, including, if necessary, the measures to mitigate any potentially adverse consequences resulting from the data breach.

The data subjects need not be informed if any of the following conditions are met:

- Le Bélier Magyarország Formaöntöde Zrt. has taken technical and organisational defence measures with regard to the data affected by the breach that will render the data incomprehensible for persons not authorised to access the personal data;
- Le Bélier Magyarország Formaöntöde Zrt. has taken further measures following the breach that ensure in all probability that the high risk to the rights and freedoms of the data subjects will not be present in the future;
- The notification would necessitate disproportionate efforts. In such cases, the data subjects must be informed by public information or similar measures must be taken to ensure their effective notification.

If Le Bélier Magyarország Formaöntöde Zrt. has not yet informed data subjects about a data breach, NAIH - after considering whether the breach carries or does not carry high risk - may order communication to the data subjects or may establish that some of the above conditions have been met.

6.2.3 Records

The person responsible for data protection shall keep records of security incidents affecting personal data or special categories of personal data in order to check the measures related to a data breach and to inform the data subjects. The records shall be kept in a table to be found in Annex 4 including the scope of personal data affected, the scope and number of data subjects affected by the data breach, the date and time, circumstances and impact of the data breach, the measures taken for its resolution, and all other information prescribed by the legal provision that requires the data processing. The content of such records shall not be modified or erased without prior written approval by the person responsible for data protection.

7 Data processing at the workplace - special rules

Le Bélier Magyarország Formaöntöde Zrt. processes the personal data of natural persons who perform work for it, including, but not exclusively, employees, temporary agency employees, trainees or sub-contractors, in the scope, for the purposes and under the legal basis specified in the records of processing activities.

Le Bélier Magyarország Formaöntöde Zrt. respects data subject rights and processes employee data only to the necessary and proportionate extent.

The following policies contain detailed rules relating to data processing at the workplace:

- (to be listed if any)

-

Data subjects shall be informed about all data processing activities described in the policies of Le Bélier Magyarország Formaöntöde Zrt. in a uniform document on the first day of their employment the latest. The privacy notice is to be found in Annex 5 so it represents a part of this Policy and 5.2.1 shall apply to its content. Data subjects shall verify that they have read and acknowledged the contents of the document by signing it. The person responsible for data protection shall review and update the information document as necessary, but at least once every year. The data subjects shall be informed of all changes affecting data processing in advance.

Le Bélier Magyarország Formaöntöde Zrt. processes employee data primarily under legal obligation or the legitimate interest of the company as the legal basis. Consent of the data subject can only be applied as a legal basis when it is clear that the natural person working for Le Bélier is in a position to make a free decision about his or her consent. In every case when Le Bélier Magyarország Formaöntöde Zrt. identifies legitimate interest as the legal basis, a balancing test shall be carried out coordinated by the person responsible for data protection, and it shall be documented in the format identified in Annex 2. As the test is carried out, special attention must be made to the relevant legal provisions as well as to the best practice of data protection.

8 Other provisions

8.1 Data quality

The processed personal data must meet the following requirements:

- their collection and processing is fair and lawful;
- they are up to date, accurate and complete;
- they allow identification of data subjects only as long as it is necessary for the purpose of their storage.

8.2 Records of controllers and processors

Le Bélier Magyarország Formaöntöde Zrt. has a duty to maintain a record of its data processing activities. The person responsible for data protection keeps the records in the format presented in Annex 1 (which includes the mandatory content of the records).

8.3 Erasure

Le Bélier Magyarország Formaöntöde Zrt. shall erase documents containing personal data once the require retention time has passed. Erasure must be executed irrecoverably, in a documented way and with the involvement of the person responsible for data protection. If this is not fully possible due to technical reasons, measures must be taken that access to the data shall be as limited as possible within Le Bélier Magyarország Formaöntöde Zrt.

8.4 Liaison with the Authority

The person responsible for data protection acts as the primary contact point for the Authority. Any oral or written communication to the Authority is made by the person responsible for data protection, or is subject to his or her approval, with the involvement of the legal function.

Any (oral or written) information received from the Authority (e.g. notification on the commencement of proceedings) shall be forwarded to the person responsible for data protection without delay.

If an officer of the Authority takes any procedural action on site as part of proceedings by the Authority, the person responsible for data protection must be present.

All persons subject to this Policy shall collaborate in proceedings by the Authority, but they are not authorised to make independent statements or direct contact. The documents requested by the

Authority shall be made available via the person responsible for data protection immediately or within the deadline specified by the person responsible for data protection.

8.5 Training

All persons subject to this Policy shall be provided with basic data protection training. The training material compiled and regularly updated by the person responsible for data protection must include, in sufficient detail, the basic concepts of data protection, the Hungarian and European legal provisions relevant to the scope of activities of Le Bélier Magyarország Formaöntöde Zrt., and the practical rules for the implementation thereof described in this Policy.

The training of new joiners shall be provided as part of their basic training at the commencement of employment, and then repeated annually. The training sessions must be documented on the attendance sheet kept by the person responsible for data protection, and training participants shall make a statement on having been made familiar with the training material. The training material must be available on the corporate intranet at all times.

If a training participant is not an employee of Le Bélier Magyarország Formaöntöde Zrt. (for instance, he or she is a sub-contractor) the person responsible for data protection may decide to deliver training in a summarised form focusing on the activity the participant will be engaged in when working for Le Bélier Magyarország Formaöntöde Zrt. (e.g. security guards). The summary form of the training should not affect compliance with data protection and data security provisions.

Annex 1: Records of processing activities



Le Bélier_Records
of processing activit

Annex 2: Legitimate interest balancing test (template)

Legitimate interest balancing test		
A. Identification of legitimate interest		
1	The purposes of the data processing	
2	Is the processing activity necessary to uphold a legitimate business interest(s)?	
3	Is the processing activity necessary to uphold a legitimate business interest(s) of a third party?	
4	Is the balancing test required under the GDPR, the Information Act, or other legal provision, or prescribed by NAIH to with respect to the processing activity?	
B. Necessity test		
1	Why is the processing activity necessary for the Controller?	
2	Why is the processing activity necessary for the third parties that can have access to the data (if any)?	
3	Can the given purpose be achieved in any other way?	
C. Balancing test		
1	Can data subjects reasonably expect that the processing activity will be performed for the given purpose?	
2	Will the processing activity provide added value to the products or services used by the data subjects?	
3	Is it possible that the processing activity has an adverse effect on data subjects' rights?	
4	Is it possible that the processing activity results in unjustified damage to data subjects?	
5	Can the Controller suffer any damage if the processing activity is not performed?	
6	Can a third party suffer any damage if the processing activity is not performed?	
7	Is the processing activity performed in the interest of data subjects (or the society)?	
8	What is the relationship between the data subjects and the organisation? (e.g. existing or prospective client, customer or supplier)	
9	Does the processing activity affect special categories of personal data as defined in the GDPR?	
10	Is there a two-way relationship between data subjects and the organisation? If yes, how regular is it (continuous, regular or occasional)?	

11	Would the processing activity impose any limitations on data subjects' rights?	
12	Have personal data been obtained from data subjects directly or indirectly?	
13	Is there an unequal relationship (subordination) between data subjects and the controller?	
14	Can data subjects reasonably expect that their personal data is processed for the given purpose? (Yes/No/Uncertain)	
15	Can data subjects consider data processing intrusive or inappropriate with respect to their privacy?	
16	Have data subjects received proper information about the processing activity and its purpose?	
17	Do data subjects have proper control over the processing activity, and can they object to it?	
18	Can the scope of the processing activity be modified to reduce/mitigate data protection risks?	
D. The guarantees and controls (e.g. privacy by design, technical and organisational measures, data minimisation, limitation of retention, restricted access, etc.) applied to protect data subjects, and mitigate risks and potentially adverse effects.		
E. Decision and reasoning (with reference to the above section)		
Date		
Name		
Position		

Annex 3: Data protection impact assessment (template)

Data protection impact assessment
Name and short description of the planned processing activity:
Persons participating in the impact assessment:
Detailed description of data processing planned under the process:
Review of the proportionality and necessity of the processing activity by the following criteria: <ul style="list-style-type: none">• identified, articulated and legitimate purpose(s);• lawfulness of data processing;• data processing is limited to the adequate, relevant and necessary data;• limited retention period.
Measures supporting data subjects' rights particularly the following: <ul style="list-style-type: none">• information provided to data subjects;• right to consultation and right to data portability;• right to rectification and erasure;• right to objection and restriction of data processing;• relationship with processors;• guarantees related to international data transfer;• preliminary consultation.
Measures planned to manage the risks affecting data subject rights and freedoms based on the assessment of the source, nature, probability, uniqueness and magnitude of the risks:
Parties involved in the data protection impact assessment:
Conclusions:
Date:
Signatures:

Annex 5: Employee Data Privacy Notice

To: All staff,

Le Bélier Magyarország Formaöntöde Zrt. takes special measures to process personal data in compliance with the legal provisions and its internal policies, and expects its employees to do so as well. The purpose of this document to inform you in detail before you start working what personal data and how Le Bélier Magyarország Formaöntöde Zrt. may process about you (about your family members in given cases) in relation to your employment.

Please read this privacy notice carefully, and if you have any questions, contact the person responsible for data protection _____ (name and position to be inserted) of Le Bélier Magyarország Formaöntöde Zrt. using any of the following means, or in person.

Telephone number:

E-mail address:

Office:

The person responsible for data protection is tasked with promoting that the rules identified in legal provisions and internal policies relating to the protection of personal data are observed. You may rest ensured that the person responsible for data protection will handle your questions, requests or complaint in confidence and – having the proper competence – will investigate them fully and take the appropriate measures if necessary. We also assure you that you will not disadvantaged as a consequence of having submitted questions, requests or complaints relating to your personal data.

In the rest of the privacy notice, the term ‘employee’ is used for the sake of simplicity. In case you will not work for Le Bélier Magyarország Formaöntöde Zrt. as an employee (for instance, on assignment or as a temporary agency employee) the provisions applying to employees shall also apply to you, *except* in the cases that are specifically connected to employment only.

This notice includes the special rules relating to the personal data of employees. Therefore, you are requested to also review **the general privacy notice in attachment or available on the website of Le Bélier** to become familiar with the general principles and rules.

What data relating to you are processed by Le Bélier Magyarország Formaöntöde Zrt.?

1. Data processed for administrative purposes in connection with your employment

Processing of the following personal data is necessary so that Le Bélier Magyarország Formaöntöde Zrt. can establish and maintain a legal relationship:

- Name, place of birth, date of birth, mother’s maiden name, tax identification, Social Security (TAJ) number, address, telephone number, salary data (fees), bank account number, tax ID, social security data, cafeteria data and data related to employee’s fitness for work.

-
- The personal data included in certificates received on leaving your previous workplace (for instance, income from previous employer and tax advance withheld).

If you intend to use certain rights and opportunities related to your employment, or wish to make use of allowances (for instance, tax allowance, paternity leave) the processing of the following may be typically necessary:

- Dependents' name, place and date of birth, tax ID and income data.
- Name, place and date of birth, tax ID, income data of spouse or life partner, data related to marriage.

The employer is authorised to process the above data by the laws related to employment (legal relationship) and taxation and social security, at the same time it has to be emphasised that legal provisions and the group of data may change or certain cases may be individually different. For instance, if you are not entitled to family tax allowance, Le Bélier Magyarország Formaöntöde Zrt. will not process the personal data required for its use (because you will not complete the relevant statement).

Therefore, the form completed or statement made by you contains in every case the group of the data required to be provided and the relevant legal provisions applicable to the given case. Therefore, you are requested to carefully read the form or statement to be completed in every case and contact the person responsible for data protection should you have any questions regarding your personal data.

Le Bélier Magyarország Formaöntöde Zrt. transfers data in compliance with the relevant legal provisions and the attached statement to the public bodies having the competence (and jurisdiction), first of all to the tax authority and the social security body.

Le Bélier Magyarország Formaöntöde Zrt. responds in compliance with legal provisions to potential claims by authorities or the court that necessitate providing personal data affecting employees (for instance, an investigating authority or bailiff).

In certain cases further data processing may arise (e.g., loan or insurance provided by employer, company events, training) in the course of which the provision of certain personal data is also necessary. In such cases, the employees involved are informed at the time data processing occurs.

Le Bélier Magyarország Formaöntöde Zrt. has outsourced payroll processing to: _____ (data processor) (only for companies where payroll services are outsourced).

Le Bélier Magyarország Formaöntöde Zrt. only processes sensitive data in limited cases: employee data (possibly data of employees' relatives) related to absence due to sickness or data related to the medical fitness of employees. Criminal personal data may be processed to respond to claims by the (investigating) authority. If special or criminal personal data are processed, the Le Bélier Magyarország Formaöntöde Zrt. pays special attention to the specific legal provisions regulating the processing of such data.

Le Bélier Magyarország Formaöntöde Zrt. retains the personal data related to employment (legal relationship) for 50 years, for 10 years in the case of payroll data, and for 5 years in the case of all

other employment-related material (retention periods specified in the Social Security Pension Benefits Act and the Labour Code are expected to be amended in the near future).

2. Data processing related to the monitoring of employees

Le Bélier Magyarország Formaöntöde Zrt. may supervise its employees' work related behaviour, while observing the relevant legal provisions and respecting their personal rights in compliance with the general authorisation provided in Section 11, Act I of 2012 on the Labour Code ("Labour Code")

With respect to persons working for Le Bélier Magyarország Formaöntöde Zrt. not in employment, the legal provisions regulating their work (for instance, Act V of 2013 on the Civil Code), the related other legal provisions and their contract concluded with Le Bélier Magyarország Formaöntöde Zrt. create the basis of supervision.

Due to its business activities, Le Bélier Magyarország Formaöntöde Zrt. needs to monitor the persons who perform work for it. Le Bélier Magyarország Formaöntöde Zrt. is committed to applying a necessary and proportionate approach to such monitoring.

The detailed rules of monitoring are identified by Le Bélier Magyarország Formaöntöde Zrt. as follows:

Data processing related to the video surveillance system operated at the Le Bélier Magyarország Formaöntöde Zrt.

In addition to the Civil Code, the rules relating to video surveillance are included in the provisions of Act CXXXIII of 2005 on the rules of personal and property protection activities and private investigation ("Security Services Act") and Act CXII of 2011 on the right of informational self-determination and the freedom of information ("Information Act"). The legal basis of data processing related to the video surveillance system is constituted by the statutory authorisation pertaining to the provisions of the laws referred to (i.e. no consent is necessary).

Subject to Section 31 (1) of the Security Services Act, the purpose of data processing is the **protection of property**.

The location of the video cameras being part of the surveillance system and the method of surveillance:

- The method of surveillance: direct surveillance of the area.
- (Description or image indicating the location of cameras to be inserted)
- The electronic surveillance system is operated by Le Bélier Magyarország Formaöntöde Zrt.
- If unused, the video recordings are stored on the server of the system for 3 days by Le Bélier Magyarország Formaöntöde Zrt. Le Bélier Magyarország Formaöntöde Zrt. stores the recordings in a closed area, controlled by special alarm and entry card system (to be inserted).
- The video recordings made by the system can only be accessed by the employees of _____ (to be inserted), the person responsible for data protection, or in the event of proceedings by the supervisory authority, the officers of the relevant authority. Recordings

can only be forwarded to them following written consent by the person responsible for data protection, and only in the event of a suspected security incident/criminal act. The staff of the reception services continuously monitors the live footage, and thereby the functioning of the system.

- The head of _____ (to be inserted) or their officers are authorised to view the recordings subsequently in justified cases and in a documented way.
- If a video recorded of an employee is used, the employee has the right to view the recording unless it hinders the investigation of a security incident/suspected criminal act, and the outcome of the potential proceedings by the authority. Further, an employee has the right to initiate with his or her line manager to obtain the opinion of the person responsible for data protection, or the modification of the settings of the security surveillance system if the security surveillance system infringes on his or her personal dignity exceeding the extent allowed by the legal provisions referred to above.
- In the event of infringements, an employee may contact the person responsible for data protection, the Hungarian National Authority for Data Protection and Freedom of Information or any other competent authority, or may turn to the court.

Electronic access control system for employees and bag search

Our company keeps records of employees entering and leaving the worksite at the reception in compliance with the provisions of the Security Services Act. As part of data processing, the electronic access control system records the employee card number, name, organisational unit and the date of entry and exit.

In addition, in the cases identified in Article 28 of the Security Services Act, on entry and exit the staff of _____ (to be inserted) may ask the employee to show the content of their bags, vehicle or cargo.

The purpose of data processing includes the records of working hours, the protection of property, the protection of persons on the premises of the company, and the protection of sensitive business information. The electronic access control system stores the recorded data for 180 days, and authorised employees of Le Bélier Magyarország Formaöntöde Zrt. and Det-Őr Kft. only have access to them for the identified data processing purpose.

Assessment of fitness for work

In compliance with the provisions of Article 52 (1) of the Labour Code and Article 60 (1) of Act XCIII of 1993 on labour safety, it is forbidden to stay or work on the premises of Le Bélier Magyarország Formaöntöde Zrt. under the influence of alcohol, or bring alcohol to the premises of our Company.

Employees are tested using a digital/electronic breath alcohol tester upon entry to the site randomly or if their behaviour indicates being under the influence of alcohol so that the labour safety requirements can be observed and their fitness for work can be assessed. The test may be carried out by the head of physical security services or the employees of Det-Őr Kft.

If the result is negative, the proceedings are closed after taking the minutes and its signature by the employee to indicate his or her acceptance.

If the result is positive, in other words the breach of policy can be established, the employee accept the result by signing the minutes, and the person performing the test must inform the line manager of the employee and the head of HR. An employee in a status unfit to work will be banned from further work on the given day, or extraordinary dismissal may take place in a justified case.

If the test is positive, but the employee challenges the result, he or she may request a blood alcohol test performed by a medical professional. The blood alcohol test will be performed by the appointed occupational physician within one hour following the original test. If the blood alcohol test is also a positive, its costs shall be borne by the employee. The result of the test must be recorded in the minutes and the Company will not provide further legal remedy.

During the procedures, the person performing the test must record in the minutes the name and ID of the employee, the name of the person performing the inspection, the time of the inspection, the result of the inspection and in given cases the fact and result of further tests. The head of Det-Őr Kft., the head of physical security services, the head of HR, the line manager of the employee, and the persons who exercise employers' rights over the employee only have the right to view the data recorded in the minutes. Le Bélier Magyarország Formaöntöde Zrt. shall retain the data processed for three years from the date of the inspection but not later than the deadline stipulated for the enforcement of claims resulting from employment, and will destroy them after that.

The undersigned _____ hereby declare to have read, understood and acknowledged the notice related to data processing at Le Bélier Magyarország Formaöntöde Zrt. at work.

Budapest, ... day month 201...

Name, position