# Information on video surveillance

## 1. Introduction

The purpose of this notice is to provide information on the Bank's processing of video surveillance in relation to data subjects (visitors, clients, prospects, employees, candidates, external service providers, suppliers, etc.) on Bank premises and elsewhere.

## 2. Data controller

The data controller for the video surveillance system is the Bank (including its branches and subsidiaries), in accordance with 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, hereinafter referred to as 'GDPR').

The Bank's registered office is located at the following address:

14, bd Royal
L-2449 Luxembourg
Telephone: (+352) 49 924-1

## 3. Contact person

If you have any questions regarding personal data protection, please contact our Data Protection Officer:

– by email at dpo@bdl.lu

– by post at the following address:

Banque de Luxembourg
For the attention of the Data Protection Officer
14 boulevard Royal
L-2449 Luxembourg

## 4. Legal basis for the processing of video surveillance

The Bank needs to process video surveillance in order to pursue legitimate interests. The legal basis is article 6(1)(f) of the GDPR.

Banque de Luxembourg only conducts video surveillance if this is necessary to protect its legitimate interests.

## 5. Purpose of the processing

The Bank processes data derived from video surveillance for security reasons, and to protect people and property.

This processing is necessary in order to:

– secure access to the Bank's premises;

– ensure the security of the Bank's staff, clients, external service providers and visitors;

– detect and identify potentially suspicious or dangerous behaviour likely to cause accidents or incidents;

– accurately ascertain the cause of an incident;

– protect Bank property (buildings, technical installations, equipment, merchandise, cash, etc.);

– organise and manage a rapid evacuation in the event of an accident;

– be able to check what has triggered a fire or intruder alarm;

– be able to alert the ambulance, fire or police services in a timely manner and facilitate their intervention.

In addition to the legitimate interests above, video surveillance (conducted in accordance with article L.261-1 of the Luxembourg Labour Code) is necessary to ensure the health and safety of staff.

Lastly, the Bank is required to conduct video surveillance of designated areas used for interactions with transporters of cash or assets, in accordance with article 29 of the Law of 12 November 2002 on private security and surveillance activities.

## 6. Data minimisation

The Bank only conducts video surveillance insofar as is strictly necessary to achieve the intended purposes (adequate, relevant and strictly necessary data) and applies the principle of proportionality to all processing operations relating to video surveillance.

## 7. Categories of processed data

Images, date, place and time recorded by surveillance cameras.

## 8. Categories of processed data recipient

As a banking institution, we are bound by professional secrecy and can only share data under strict conditions.

The Bank may be obliged to share data with its processors in accordance with the law and for the sole purpose of providing the services for which they have been contracted.

The Bank is also required to share data in instances where professional secrecy is waived by the law, including with the police or competent legal authorities in the context of a criminal procedure, or another type of procedure if the Bank needs to protect its interests in court.

The images may therefore be seen, in the event of an incident or offence, by duly authorised personnel and by the police or competent legal authorities.

Your data shall remain in Luxembourg in the European Union and shall not be transferred to a third country under any circumstances.

## 9. Data retention period

Data derived from video surveillance is kept for a maximum period of 30 days. However, the data retention period may be extended in the event of an incident, offence or ongoing legal proceedings. This data will then be deleted without undue delay if it is no longer needed to achieve the aim for which it was collected.

This retention period is justified by the Bank's activity, the risks inherent in this activity (for visitors, staff and, more broadly, anyone present on Bank premises) and the need to have sufficient time to professionally review and investigate criminal activities, incidents or complaints such as:

– fraudulent or criminal use of payment methods;

– theft or misappropriation of funds;

– reconnaissance of the premises before a burglary or other criminal operation;

– armed aggression or attack;

– vandalism.

## 10. Transparency

When the Bank conducts video surveillance, data subjects are informed of this by means of signs and pictograms in areas where video surveillance is in use, as well as a more detailed information notice available on the Bank's website at https://www.banquedeluxembourg.com/en/bank/bl/data-protection?country=LU

## 11. Documentation

The Bank lists and documents each video surveillance system in accordance with personal data protection requirements.

## 12. Data protection

The Bank has established suitable technical and organisational measures to guarantee the security and confidentiality of the data being processed.

## 13. Your rights

Subject to the conditions and limits stipulated by the legislative and regulatory provisions, data subjects have a certain number of rights regarding the processing of their personal data. Please contact our Data Protection Officer with any requests in this regard.

Firstly, you have a right to information and are therefore entitled to receive further information not included in this notice.

You also have the right to ask the Bank for access to your personal data, the right to rectify or erase such data, the right to limit processing in relation to the data subject, the right to object to data processing and the right to data portability.

To enable you to exercise your rights, we may ask you to state the data/processing operations/period and/or exact location to which your request relates before providing the data.

The person making the request will need to provide a copy of their identity document so that their request can be processed, and for identification purposes.

## 14. Automated decision-making including profiling

The Bank hereby confirms that it does not engage in automated decision-making including profiling.

## 15. Complaints

If you feel that your data has not been processed in accordance with the GDPR, you can file a complaint with our Data Protection Officer.

You also have the right to make a complaint regarding the Bank's processing of your personal data with the National Commission for Data Protection on the website https://cnpd.public.lu/en/particuliers/faire-valoir/formulaire-plainte.html or by post:

Commission nationale pour la protection des données
Service des réclamations
15, Boulevard du Jazz
L-4370 Belvaux

## 16. Updates

This information notice may be amended to ensure better protection of your personal data. The latest version is available on the Bank's website.