Privacy statement

1. Purpose

In order to enable you to use the Website, LBC Tank Terminals ("LBC", "we", "us", "our", "ours") processes ("Processing" meaning: all possible operations on data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, combination, restriction, erasure or destruction) information about you ("Personal Data") in accordance with the below provisions.

LBC is strongly committed to privacy and personal data protection. We respect your rights under the European General Data Protection Regulation ("GDPR") (and all other local legislations that might be applicable) and comply with all of the requirements in respect of the Processing of your Personal Data. This privacy policy explains how LBC processes your Personal Data when you navigate on the Website.

2. Who is involved in the Processing of your Personal Data?

2.1. For the Processing of your Personal Data through the Website, LBC acts as the data controller with respect to your Personal Data, which means that we determine the purposes and means of the Processing of your Personal Data and will be the first responsible for ensuring that this is done in a lawful and secure manner.

LBC Belgium Holding NV with registered office at Schaliënhoevedreef 20E, 2800 Mechelen, Belgium (corporate registration number 0865.098.557)

2.2. LBC guarantees that any person acting under its authority and having access to your Personal Data (e.g. LBC employees), only Processes your Personal Data in accordance with LBC's instructions and have in particular committed themselves to confidentiality.

2.3. LBC may engage sub-contractors (Processors) with respect to the Processing of your Personal Data (e.g. website developers or hosting service providers). LBC ensures to only engage sub-contractors providing sufficient guarantees towards the lawful Processing and security of your Personal Data.

2.4. LBC may share your Personal Data with any entities part of the LBC group in order to provide our services in a successful and qualitative manner.

2.5. LBC may transfer your Personal Data outside the European Economic Area. For transfers outside of the EEA, LBC will ensure an adequacy decision by the European Commission is in place for the recipient country or organisation, or that appropriate or suitable safeguards are in place, a copy of which can be obtained by contacting LBC (please see our contact details below).

3. Which Personal Data will be Processed, for what purposes and for how long?

3.1. Through the Website, we will gather the following categories of Personal Data:

- Identification data
- Professional data
- Electronic identification data

In addition to the above categories of Personal Data, we may process any other type of Personal Data you voluntarily provide to us during your visit of the Website or the information we deduce from your use of the Website.

3.2. We will Process your Personal Data in order to be able to respond to any queries you may send us through the Website (the "Purpose").

Prior to using user data for other purposes, LBC will update this statement to inform you of such changes and your rights in view of such changes.

3.3. We will only Process your Personal Data for as long as it is necessary for the Purpose listed above.

4. What rights do you have with respect to your Personal Data?

4.1. LBC will implement appropriate technical and organisational measures to ensure that the Processing of your Personal Data is performed in accordance with data protection law, in particular ensuring an appropriate level of security to protect your Personal Data from loss, misuse, alteration or destruction.

4.2. By contacting us (please see our contact details below), you may, at any time request (with an acceptable proof of identity):

- confirmation as to whether or not Personal Data concerning you are being processed by us and, where that is the case, you may request access to or receipt of your Personal Data;
- to rectify inaccurate Personal Data concerning you;
- to complete incomplete Personal Data concerning you;
- to erase or to restrict the Processing of (certain) Personal Data relating to you;
- to transmit your Personal Data to another controller or processor; and
- to cease the Processing of your Personal Data.

We will investigate whether it is feasible to respond to your request and whether we are legally obliged to do so. We will give you written confirmation about the chosen way forward.

5. Any further questions or complaints with respect to the Processing of your Personal Data?

5.1. In case you have any questions with respect to the Processing of your Personal Data, you can contact us by e-mail (data.protection@lbctt.com).

5.2. Please note that you have the right to lodge a complaint with a supervisory authority of your choice at any time if you are of the opinion that the Processing of your Personal Data by LBC infringes the GDPR.

Data Protection policy

1. Purpose

LBC collects and uses personal data to provide world-class services for our employees, clients, and partners. This Data Protection Policy (the 'Policy') is designed to set forth how LBC will handle Personal Data that it collects or otherwise Processes in the normal course of business. LBC strives to be global and consistent in how it handles Personal Data. This Policy applies to:

1. All individuals who provide personal information, such as clients, business partners, suppliers, shareholders, or their respective representatives, job applicants, employees, retirees and others;
2. All locations where LBC operates, even where local regulations do not exist; and

3. All methods of contact, including in person, written, via the Internet, direct mail, telephone, or facsimile.

This Policy describes LBC's standard global procedure governing access to and use of Personal Data across borders. As part of this Policy, LBC will comply in all material respects with the European 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") and implementing legislation enacted by the member states of the European Union with respect to its operations in those member states; as well as other privacy laws, rules, and regulations that may apply to LBC, its employees, or its clients in those countries where LBC has operations ('Data Protection Law').

This Policy does not necessarily describe how local management may handle Personal Data in order to comply with local privacy laws. Local management in conjunction with the responsible human resources manager(s) will be responsible for accessing and complying with local/unique laws and/or rules regarding the processing of Personal Data in that particular locale.

This Policy is also designed to inform all employees about their obligation to protect the privacy of all individuals (whether co-employees, independent contractors, or sub-contractors) and the security of their Personal Data. The violation of this Policy, whether negligent or intentional, will be subject to disciplinary action by LBC.

2. Scope

This is a Global Policy. LBC will implement the applicable principles under the General Data Protection Regulation to all Personal Data transferred outside of the European Union. LBC facilities are required to comply with this Policy as well as with the privacy laws in force in their local jurisdictions.

3. Responsibility and authority.

The Privacy Office will consist of a representative from the IT, Legal, HR and Corporate Social Responsibility (CSR) departments.

3.1. IT: to establish and maintain an IT environment compliant with this Policy and the applicable Data Protection Law by doing regular audits, maintaining an up to date data flow chart and restricting the rights of access to Personal Data as much as operationally possible both for LBC employees and external contractors or application providers.

3.2. Legal: to advice and to assist with issues arising from this Policy or compliance with Data Protection Law.

3.3. HR: to be the first line of response when LBC employees submit questions or concerns with respect to this Policy or other data protection issues. To assure compliance with this Policy and the applicable Data Protection Law regarding personnel files.

3.4. CSR: to establish and enforce a clear and auditable process to assess the compliance by all employees, departments and entities within the LBC group, and where applicable contractors, with this Policy and the procedures relating to this Policy. To assure compliance with this Policy and the applicable Data Protection Law regarding security registers and rights of access data files.

No Data Protection Officer (in the meaning of article 37 of the GDPR) has been appointed taking into account that LBC's core activities are considered not to fall within the scope of application of article 37 of the GDPR. For further information please consult the LBC Privacy Office(r).

4. Definitions

Definitions pertaining to this policy are:

4.1. **"Controller,"** in this case, refers to LBC and its authorized representatives, which determine the purposes and means of processing of Personal Data.

4.2. **"Supervisory Authority",** also commonly referred to "Data Protection Authority", means the local, national or international authority competent to monitor and enforce compliance with applicable data protection law.

4.3. **"Data Subject"** in this case refers to any employee or third person (e.g., client's representative, consultant or independent contractor) who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

4.4. **"General Business Purpose"** means any activity related to the commercial and business operations and activities of LBC's worldwide organization. This could include, but is not limited to its operations, sales, marketing, and research and development operations; protecting intellectual property; the provision of services; internal operations; and general employment matters, including recruitment both internally and externally. Data Processing for General Business Purposes includes, but is not limited to, operational security, maintaining files, payroll processing, managing benefit and medical plans, conducting performance reviews, and intra-company communications.

4.5. **"Personal Data"** means any information related to an identified or an identifiable person. For example, a Data Subject's home address, e-mail address and/or phone number, personnel file, or benefits information would constitute Personal Data.

4.6. **"Sensitive Data"** is a subset of Personal Data and refers to any Personal Data pertaining to racial or ethnic origins, trade union membership, medical or health conditions, political or religious beliefs, sex life, or criminal history.

4.7. **"Processor"** means a natural or legal person, or any other entity that processes Personal Data on behalf of the Controller and under its control. In this context, a Processor may be an external payroll preparation firm that works on behalf of LBC and under its control or an LBC entity providing intragroup services (e.g. LBC Belgium Holding NV). LBC requires external and internal Processors to protect the privacy, confidentiality and security of LBC's Personal Data.

4.8. **"Processing"** of Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

4.9. **"Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (e.g. loss of a PC or mobile device, LBC documents incl. Personal Data or sending e-mails to wrong addressees).

4.10. **"LBC"** means LBC Belgium Holding NV, as well as its affiliated and subsidiary companies within the group.

4.11. **"Third Party"** means any natural or legal person, public authority, agency or any other entity other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data.

4.12. **"Privacy Office(r)"** means the office/officer in charge for providing LBC as well as all addressees of this Policy technical or practical guidance with respect to the implementation

and application of this Policy, as well as to support with respect to any questions related to the processing of personal data and the protection of privacy.

5. Standard Minimum Requirements of the Policy

5.1. Quality of Personal Data

LBC, with guidance from the Privacy Office(r), will take reasonable steps to ensure that all Personal Data are:

a) Obtained, where possible, directly from the Data Subject to whom the Personal Data relates;

b) Obtained and Processed fairly and lawfully by LBC for General Business Purposes;

c) Relevant to and no more revealing than is necessary for General Business Purposes; and

d) Kept up to date to maintain data accuracy, while data are under the control of LBC, and kept only for so long as is reasonably necessary.

5.2. Lawfulness of the Processing

LBC will only Process Personal Data to the extent that there is a sufficient legal basis which allows the envisaged Processing of the Personal Data. Following can constitute a legal basis:

a) the Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

b) the Processing is necessary for compliance by LBC with a legal obligation to which it is bound;

c) the Processing is necessary to protect the vital interests of the Data Subject or another natural person;

d) the Processing is necessary by virtue of the legitimate interest pursued by LBC or a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject;

e) the Data Subject has given consent to the processing of his/her Personal Data for the envisaged purposes. In case consent is sought from the Data Subject, such consent, incl. the terms based upon which consent was obtained and the process used to obtain such consent (incl. a time-stamp) should be documented

Please note that HR related Processing activities should not be based on consent. Seeking and relying on employee consent is restricted to specific circumstances and should not be done without seeking prior guidance from the Privacy Office(r).

5.3. Notice and Use of Personal Data

LBC will not collect or otherwise Process Personal Data in a manner that is deceptive, misleading, fraudulent, or dishonest or which would in any other way constitute a breach of applicable Data Protection Law.

When required, LBC informs Data Subjects what information it collects, how it is used, whether it may be temporarily transferred to others to provide the products or services requested and how to contact LBC with privacy inquiries.

LBC takes reasonable steps to provide the Data Subject with the following minimum information prior to the collection (unless the Data Subject has already received this information):

a) The identity and contact details of the LBC entity qualifying as Data Controller for the Processing;

b) The contact details of the Privacy Office(r);

c) The purposes and the applicable legal basis for the Processing (as the case may be specifying the legitimate interest pursued by LBC);

d) Where applicable, the fact that the Company intends to transfer Personal Data to a country outside the EEA with reference to the appropriate safeguards in place and the means available to obtain a copy of such safeguards;

e) (the categories) of recipients of the Processed Personal Data;

f) the period for which the Personal Data is retained, or if that is not possible, the criteria used to determine this period;

g) The Data Subject's rights, incl. the right to request access to and rectification or erasure of their Personal Data, the right to request the restriction of or object to the Processing of their Personal Data, where applicable, the right to withdraw consent and the right to data portability;

h) How Data Subjects can exercise their rights, incl. the right to lodge a complaint with a Supervisory Authority;

i) Where applicable, the existence of automated decision making, incl. profiling, as well as the significance and the envisaged consequences of such Processing for the Data Subjects;

If Personal Data is not obtained directly from the Data Subject (e.g. through a client), the entity qualifying as Controller must ensure the information is provided through other means to the Data Subject, for instance by requesting sufficient comfort (e.g. contractual warranty) from a client that the data has been lawfully collected and that the necessary information has been provided to the relevant data subjects unless the Processing is authorized or required by law or where the provision of such information would prove impossible or would involve a disproportionate effort for the Company. In this last case, appropriate measures should be taken to protect the rights and freedoms and interests of the Data Subject, including making the information publicly available.

5.4. Data Minimisation

LBC's use of Personal Data will be limited to General Business Purposes and will not be kept longer than is necessary.

Personal Data shall be retained in accordance with the retention policy and periods set out by LBC.

Where collection and Processing would be done for other purposes or for longer periods of time, please contact LBC's Privacy Office(r) via e-mail (data.protection@lbctt.com) for further guidance.

5.5. Data Retention

Law, business practice and trade custom provide for a number of different retention periods. In order to meet the mandatory data retention periods and also take into account possible maximum retention periods, LBC shall implement appropriate data management measures.

Unless a longer or shorter retention period is required by law (e.g. data privacy laws) or for other reasons (e.g. legitimate business needs), the standard retention period applying to all LBC data shall be ten (10) years.

The retention period starts

a) if data relates to a contract with continuous obligations (e.g. a multi-year supply contract, a non-disclosure agreement, a long-term lease) or a long-term activity (e.g. multi-year projects): on January 1st of the year that directly follows the year in which the long-term activity or all contractual obligations are terminated;

b) if data relates to legal proceedings or disputes: on January 1st of the year that directly follows the year in which the legal proceedings ended;

c) if data is created for internal purposes (e.g. meeting minutes, memos): on January 1st of the year that directly follows the year in which the data was created;

d) if the respective data was created as an external communication or a combination of internal and external communication (e.g. business letter, minutes on meeting with a supplier/customer): on January 1st of the year that directly follows the year in which data was created and sent by LBC to a third party; until the Data is sent c) applies, or

e) if data was received or otherwise obtained by LBC from a third party (including other companies of the LBC group), irrespective of whether the data was requested, involuntarily received or otherwise obtained: on January 1st of the year that directly follows the year in which data was received/obtained; or

Drafts, previous versions and duplicate copies can be deleted immediately unless the storage of those is required by law.

5.6. Data destruction

Data shall be destroyed upon the expiration of the applicable retention period by LBC, following prior consultation with the Privacy Office(r) to verify whether or not the data must be subject to data preservation (e.g. because an investigation is pending).

Personnel assigned by LBC shall carry out the destruction as soon as reasonably practicable following the expiration of the retention period. Data that is subject to a data preservation shall only be destroyed, once the data preservation is released.

If data is stored with Third Parties, LBC shall instruct and monitor the deletion/destruction with the Third Party and request documentation of deletion/destruction of data.

Personnel carrying out the destruction shall maintain a record of the destruction.

5.7. Specifics for Personal Data

If a data set comprises several categories of Personal Data that are subject to different retention periods, any Personal Data subject to a shorter retention period must be removed from that data set at the end of the respective retention period.

To the extent that Personal Data is stored in different IT-systems, it must be deleted from one IT-system if it is not needed anymore for the purpose of that specific IT-system.

The processing of Personal Data must further be restricted even within the retention period when

a) the data subject requests the erasure of Personal Data concerning him/her but processing of that Data is necessary for compliance with a legal obligation under Art. 17 para. 3 GDPR, or

b) the data subject requests the restriction of processing in accordance with Art. 18 GDPR.

Restriction of processing means the marking of data with the aim of limiting their processing in the future. If a restriction of the processing of Personal Data is required, access to that data must be limited to personnel that need access to fulfil the task(s) that prevented deletion of that data.

Rather than erasing/deleting Personal Data, data may also be kept in an anonymized form if there are reasonable grounds for such an anonymization (e.g. further use of data for statistical analyses). Yet anonymized data is also subject to the data retention periods established above.

Any process of anonymisation of Data has to be aligned with the Privacy Office(r).

5.8. Individual Rights of Data Subjects

LBC takes steps to make sure that the Personal Data it uses is correct. LBC will allow Data Subjects reasonable access to Personal Data about themselves during normal working hours and upon reasonable request and will be allowed to update and/or correct any inaccurate information.

Such requests are subject to specific conditions which should be analysed before responding to a request, therefore all such requests as well as all other requests from Data Subjects should upon receipt be directed to LBC's Privacy Office(r) via e-mail (data.protection@lbctt.com).

5.9. Third Party Access Requests or Governmental requests

Similarly, any Third-Party request or governmental request with respect to the Processing of Personal Data within LBC should upon receipt be directed to LBC's Privacy Office(r) via e-mail (data.protection@lbctt.com).

5.10. Security of Personal Data

LBC will take reasonable precautions to protect Personal Data and, in particular for Sensitive Data, from loss, misuse, unauthorized access, disclosure, alteration and destruction. For these purposes, LBC will implement appropriate technical and organizational measures appropriate to the risk for the Data Subject. For further information, please contact LBC's - IT responsible via e-mail i-haleydt@lbctt.com

5.11. Data Protection Impact Assessment

Where the Processing is likely to result in a high risk to the rights and freedoms of the Data Subject, a Data Protection Impact Assessment must be performed. When required by applicable Data Protection Law, the competent Supervisory Authority must be consulted prior to initiating the Processing.

For further guidance on this obligation, the methodology and template for such Data Protection Impact Assessments (incl. the necessary questions to help you assess whether the envisaged processing is likely to result in a high for Data Subjects), please consult LBC's Privacy Office(r) via e-mail (data.protection@lbctt.com).

In any case, LBC imposes that a DPIA is performed when following Processing is envisaged:

- The Processing includes automated-decision making, incl. profiling;
- The Processing includes Sensitive Data;
- The Processing includes the monitoring of a publicly accessible area;
- The Processing involves the development or implementation of new technologies (e.g. the implementation of a new cloud-based application, the automation or digitization of a process involving substantive Personal Data);
- The Processing relates to a group or business reorganization within LBC;

Where a possible change in risk is identified for the Processing activities for which the DPIA has been performed, LBC will perform a review to assess whether the Processing is still performed in accordance with the DPIA.

5.12. Transfers of Personal Data

LBC may from time to time transfer Personal Data within and between its various worldwide locations as well as to Third Parties for General Business Purposes, in compliance with country of origin regulations, other applicable Data Protection Law and this Policy.

LBC's personnel, outside firms and consultants, and clients who receive Personal Data may be located in the Data Subject's home country, the EU, the United States of America or any other country in which LBC does business. Therefore, Personal Data may be transferred to any country in the world, including but not limited to the EU, the United States of America, and other countries where LBC does business, and where the privacy laws may be more or less protective than the privacy laws where the Data Subjects live or work.

Concerned individuals may withhold their consent to such international transfers and are to be informed of the impact such opt-out will have on their business relationship with LBC (e.g. inability to deliver services).

Personal Data transfers should meet the applicable requirements under Data Protection Law, in particular where transfers take place to Third Parties or to countries outside of the country where the respective LBC entity is located (whether intragroup or not).

Transfers must at all times be governed by a data processing contract (cf. Standard contractual clauses as adopted by the European Commission, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF). Data processing contracts should be submitted to the Legal Department at least 10 Business Days in advance for review and validation prior to conclusion.

5.13. Accountability

LBC must be able to demonstrate compliance with applicable Data Protection Law and this Policy.

LBC maintains records of its Processing activities in electronic form. These records maintain at least the following information:

- The name and contact details of LBC and where applicable those of the joint-Controller and the data protection officer;
- The purposes of the Processing;
- A description of the categories of Data Subjects and of the Processed Personal Data;
- The categories of recipients to whom the Personal Data will be disclosed;
- Where applicable, the transfer of the Personal Data to countries outside the European Union and, in such case, with reference to the appropriate safeguards in place and the means available to obtain a copy of such safeguards;
- Where possible, the envisaged retention period of the Personal Data;
- Where possible, a description of the technical and organizational measures.

When new Processing or a change to current Processing is envisaged by LBC, the necessary information allowing for the update of the LBC records and for an analysis of the possible application of other obligations to LBC, following the new or changed Processing, should be provided to LBC's Privacy Office(r) via e-mail (data.protection@lbctt.com).

LBC expects its employees, independent contractors, subcontractors, and partners to maintain the trust placed in LBC by those Data Subjects who provide Personal Data to LBC. LBC will provide privacy training to its employees to highlight the importance of privacy in its global business conduct program, how to lawfully Process Personal Data in the context of their activities and how to deal with possible incidents, claims or other requests from stakeholders.

Those who manage Personal Data will complete periodic privacy self-assessments to make sure that Personal Data is secure and protected. LBC will periodically audit and stress-test privacy compliance and where necessary, will extend by contract its privacy policies and data protection practices to LBC's supplier and partner relationships.

5.14. Data Protection Breach Management Plan

Managing Data Breaches is important to protect the Personal Data of Data Subjects when a Data Breach occurs. LBC has therefore established an effective and comprehensive Data Protection Breach Management Plan, including the necessary steps to take, such as, where applicable, the mandatory notification to the Supervisory Authority within 72 hours or other required deadlines. For further information please contact the Privacy Office(r) via e-mail (data.protection@lbctt.com).

LBC will continuously review this Data Protection Breach Management Plan to ensure it remains effective and relevant as business operations evolve. LBC will also register Data Breaches in the LBC Data Breach Register. All (suspected) Data Breaches should be communicated without any delay to the Privacy Office(r) via e-mail (data.protection@lbctt.com).

5.15. Status of Policy

This Policy is subject to change, although LBC will provide updates from time to time about changes to this Policy. In case of the sale of the company, acquisition or merger, bankruptcy or other change in corporate status, this Policy could change. In addition, this Policy may be supplemented by other company policies and statements.

5.16. For More Information

Questions or concerns about how LBC handles Personal Data, are to be directed to the following address data.protection@lbctt.com.

6. Annex 1 – Data Protection Breach Management Plan

The following four key activities are to be taken when a Data Breach is being detected:

Containment and recovery

Assessment of ongoing risk

Reporting of Breach

Evaluation and response

1. Containing the Breach

ACTIONS	CHECK
• Alert the Data Breach management team at data.protection@lbctt.com • The Data Breach management team will consist of a representative from the IT, Legal, HR and Corporate Social Responsibility department.	
• Unless otherwise instructed by the Data Breach management team, shut down the compromised system that led to the Data Breach.	

• Put a stop to practices that led to the Data Breach.	
• Establish whether steps can be taken to recover lost data and limit any damage caused by the Breach.	
• Isolate the causes of the Data Breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system. Where needed, replace the affected systems or infrastructure.	
• Prevent further unauthorized access to the system. Reset passwords if accounts and passwords have been compromised. Stress test prior to going live.	
• Notify the police or competent cybercrime unit if criminal activity is suspected and preserve evidence for investigation.	

2. Assessing Risks and Impact

Risk and impact on individuals	check or complete
• What is the nature of the Breach? How many Data Subjects were affected? *A higher number may not mean a higher risk, but assessing this helps overall risk assessment.*	
• Whose Personal Data had been breached? *Does the Personal Data belong to employees, customers or minors? Different people will face varying levels of risk as a result of a loss of Personal Data.*	
• What types of Personal Data were involved? What is the approximate number of data records concerned? *This will help to ascertain if there are risk to reputation, identity theft, safety and/or financial loss of affected individuals.*	
• Any additional measures in place to minimize the impact of a Data Breach? *E.g. a lost device protected by a strong password or encryption could reduce the impact of a Data Breach.*	

Risk and Impact on Organizations	
• What caused the Data Breach? *Determining how the Breach occurred (through theft, accident, unauthorized access, etc.) will help organizations identify immediate steps to take to contain the Breach and restore public confidence in a product or service.*	
• When and how often did the Breach occur? *Examining this will help organizations better understand the nature of the Breach (e.g. malicious or accidental).*	
• Who might gain access to the compromised Personal Data? *This will ascertain how the compromised data could be used. In particular notification to affected individuals would be required if personal data is acquired by an unauthorized person.*	
• Will compromised data affect transactions with any other Third Parties? *Determining this will help identify if other organizations need to be notified.*	
• What is the risk for the affected Data Subjects? Does it qualify as a high risk?	

3. Reporting the Breach

• Register the Breach in the LBC Breach register	
WHO to Notify	check or complete
• When required, notify the competent Data Protection Authorities within the required deadlines (in EU: if the Breach is likely to result in a risk to the rights and freedoms of Data Subjects)	
• When required, notify Data Subjects whose Personal Data has been compromised (in EU: if the Breach is likely to result in a high risk to the rights and freedoms of Data Subjects). This includes guardians or parents of young children whose Personal Data has been compromised.	
• Notify other Third Parties such as banks, credit card companies or the police, where relevant.	

WHEN to Notify	
• Notify the competent data protection authorities in EU within 72 hours. If this is not possible, notify the data protection authorities within such timeframe with the reasons of delay.	
• Notify affected individuals immediately if a Data Breach involves sensitive personal data or is otherwise likely to result in a high risk for the individual. This allows them to take necessary actions early to avoid potential abuse of the compromised data.	
• Notify affected Data Subjects when the Data Breach is resolved.	
HOW to Notify	
• Adopt the most effective ways to reach out to affected Data Subjects, taking into consideration the urgency of the situation and number of Data Subjects affected (e.g. media releases, social media, e-mails, telephone calls, faxes and letters).	
• Notifications should be simple to understand, specific and provide clear instructions on what Data Subjects can do to protect themselves.	
WHAT to Notify	
• To Supervisory Authority: Nature of the Personal Data Breach including where possible ✓ how and when the Data Breach occurred; ✓ types and approximate number of Personal Data involved in the Data Breach; ✓ categories and approximate number of Data Subjects concerned.	

• To Supervisory Authority and concerned Data Subject: ✓ What the organisation has done or will be doing in response to the risks brought about by the Data Breach; ✓ Specific facts on the Data Breach and likely consequences of the Personal Data Breach where applicable; ✓ Actions Data Subjects can take to prevent their Personal Data from being misused or abused; ✓ Contact details and how affected Data Subjects can reach the organization (data protection officer or contact point) for further information or assistance (e.g. helpline numbers, e-mail addresses or websites).	

4. Evaluation and Response

After steps have been taken to resolve the Data Breach following the steps described above, the Privacy Office(r), as the case may be together with the concerned department, shall review the cause of the Breach and evaluate if existing protection and prevention measures are sufficient to prevent similar Breaches from occurring. Follow-up with the competent Supervisory Authority, police or cybercrime unit where relevant. The review shall consider the following areas and write down an extensive report containing the following items:

Operational and Policy Related Issues	check or complete
• Were audits regularly conducted on both physical and IT-related security measures? • Are there processes that can be streamlined or introduced to limit the damage if future Breaches happen or to prevent a relapse? • Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices or connectivity to the Internet? • Were the methods for accessing and transmitting Personal Data sufficiently secure, e.g., access limited to authorised personnel only? • Should support services from external parties be enhanced, such as vendors and partners, to better protect Personal Data? • Were the responsibilities of vendors and partners clearly defined in relation to the handling of Personal Data? • Is there a need to develop new Data-Breach scenarios?	

Resource Related Issues	
• Were there enough resources to manage the Data Breach? Should external resources be engaged to better manage such incidents? • Were key personnel given sufficient resources to manage the incident?	
Employee Related Issues	
• Were employees aware of security related issues? • Was training provided on Personal Data protection matters and incident management skills? • Were employees informed of the Data Breach and the learning points from the incident?	
Management Related Issues	
• How was management involved in the management of the Data Breach? • Was there a clear line of responsibility and communication during the management of the Data Breach?	