Modern Expo

General Information Security and Data Breach Policy

Title	General Information Security and Data Breach Policy
Organization	Modern-Expo B.V.
Policy version	v. 1
Effective Date	31.12. 2019
Last Review Date	31.12. 2019
Next Review Date	31.12.2020
Owner	The Group Legal Office
For questions about this Policy, contact:	The Group Legal Office at legal@modern-expo.com

Contents

Part A. General

1. Scope

This Policy applies to all directors, managers, employees, contractors and any other workers (each, an "**Employee**") within our organisation and its affiliates and subsidiaries ("**Modern Expo**", "**we**," "**us**") with respect to all operations carried out by Modern Expo around the world which involve the processing of personal data.

References to "Modern Expo" or "us" are to each relevant Modern Expo entity. Each Modern Expo entity has adopted this Policy as its own Information Security and Data Breach Policy. This Policy applies in respect of certain Modern Expo entities with such variations (to reflect e.g. local laws) as may be specified in the relevant local annexes to this Policy (if any).

This Policy complements the General Privacy Policy and other Modern Expo policies and procedures.

2. Enforcement

It is the responsibility of every Employee to comply with this Policy. Acknowledgment and understanding of this Policy is required through contracts and mandatory training. Failure to comply with this Policy may be a breach of the terms of employment and may lead to disciplinary actions up to and including termination of employment or services contracts.

3. Amendments to this Policy

The Group Legal Office will review this policy no less than once every year and recommend any appropriate changes.

4. Exceptions

Any exception to this Policy must be approved in writing by the highest management of the relevant Modern Expo entity (who will ordinarily seek the advice of the Group Legal Office). All exceptions to this Policy must be approved before implementation.

5. Useful Contacts

Function	**Contact details**
Report a suspected data breach	**databreach@modern-expo.com**
Information Security Officer	**ISO@modern-expo.com**
Data Privacy Team	**privacy@modern-expo.com**

Part B. Information Security Policy

1. Information security principles

1.1. Principles each Employee must follow

Each Employee and business function must seek to implement the following information security principles within their area of activity:

(a) prevent unauthorized access to or unauthorized use of personal information;

(b) restrict the storage, access and transportation of records containing personal information outside of business premises;

(c) prevent terminated Employees from accessing business premises, and records containing personal data;

(d) implement restrictions on physical access to records containing personal information, and store such records in locked facilities or containers;

(e) educate and train Employees about the importance of personal information security;

(f) store information and physical records in a manner that provides protection and security to a degree proportional to their importance and sensitivity. For example, important physical records should be stored in a fire proof safe or vault.

(g) seek approval of the IT and Information Security Office for changes in business practices that may impact on information security.

In particular, unless permitted in accordance with a written operating procedure (or by the ISO in writing):

(i) do not tell or disclose your passwords to anyone else;

(ii) make sure you lock the screen of your computer (with a password) each time you stand up from your workplace;

(iii) do not discuss confidential information (including personal data) with anyone, except as needed for business purposes;

(iv) do not keep work files on your personal devices;

(v) maintain a clean desk policy; remove all paper documents that you do not work with right now;

(vi) do not leave documents unattended in common areas (such as a meeting room or canteen);

(vii) do not allow strangers to enter Modern Expo premises;

(viii) do not use flash drives or any other external storage for any business data.

1.2. Principles IT staff must follow

The IT staff, including the members of the IT and Information Security Office, must implement the following information security principles:

(a) ensure that each computer and network application has secure user authentication protocols, including:

(i) control of user IDs and other identifiers;

(ii) a secure method of assigning and selecting passwords, or use of unique identifier technologies;

(iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(iv) restricting access to active users and active user accounts only;

(v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system; and

(vi) making sure the screens of all computers are automatically locked with a password after one minute of inactivity (unless otherwise provided for in ISO's operating procedures).

(b) ensure that each computer and network application has secure access control measures that:

(i) restrict access to records and files containing personal data to those who need such data to perform their job duties; and

(ii) assign unique identifications and passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

(c) encrypt all personal data, however processed, and whenever possible. For example, encrypt:

(i) all information that will travel across public networks or be transmitted wirelessly;

(ii) all data stored on computers, laptops and other portable devices;

(d) ensure that data is backed up and protected from accidental loss, corruption or inaccessibility;

(e) monitor systems for unauthorized use of or access to personal data;

(f) ensure that each system that is connected to the Internet has an up-to-date firewall protection and operating system security patches;

(g) ensure that each system has up-to-date versions of system security agent software which must include malware protection and up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis;

(h) ensure that IT equipment that is disposed of does not contain personal data;

(i) ensure that staff knows how to irretrievably delete information (and that appropriate "secure deletion" tools are installed at all systems where needed);

(j) educate and train Employees on the proper use of the computer security systems.

2. Information Security Officer

The head of the Group IT and Information Security Office will designate the Information Security Officer of each Modern Expo entity ("**ISO**") or, in the absence of such designation, will carry out the role of the ISO. The ISO will be responsible for information security within each Modern Expo entity.

The ISO can be reached at **ISO@modern-expo.com**.

The ISO will keep this Policy under regular review and will notify the Group Legal Office and the management of the relevant Modern Expo entity whenever updates to this Policy are needed.

3. Audits and risk assessments

The ISO will carry out regular audits relating to the reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of any electronic, paper or other records containing personal data. The audits will be carried out not least than annually and reports on such audits will be sent to the highest management and the Group Legal Office.

The ISO will evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

(a) issuing and updating operating procedures;

(b) ongoing training for Employees;

(c) enforcing breaches of policies and procedures; and

(d) upgrading technological safeguards and means for detecting and preventing security system failures.

Following each incident involving a breach of security, the ISO will conduct mandatory post-incident review of events and actions taken, if any, and recommend changes in business practices relating to protection of personal data.

4. Operating procedures

The ISO will prepare operating procedures for Modern Expo Employees relating to information security and recommend those for approval by the highest management of the relevant Modern Expo entity.

The operating procedures will detail and implement the information security principles listed in section 1 above.

5. Vendor diligence

The ISO will be responsible for ensuring that Modern Expo's vendors who may process personal data on behalf of Modern Expo ("**data processors**") have implemented appropriate technical measures to ensure security of personal data.

For this purpose, the ISO will carry out due diligence on the data processor's information security measures before such vendor is engaged by Modern Expo. After engagement, the ISO will keep the vendor's information security measures under regular review.

The ISO will make recommendations to the Legal Office from time to time as to any specific obligations to be undertaken by vendors in respect of implementing and maintaining appropriate information security measures for safeguarding personal data.

Part C. Data Breach Policy

1. Purpose

This Data Breach Policy identifies the procedures that Modern Expo will follow in the event of an actual, potential or suspected Data Security Incident (as defined below in 2.2).

2. Incident Reporting Requirement

2.1 Report All Incidents

Any Employee that discovers, suspects, or otherwise learns about an actual, potential or suspected Data Security Incident (see next section) must immediately report it by sending an email to **databreach@modern-expo.com**.

See Appendix A for a sample Data Security Incident Reporting Form that is recommended to be used by the reporting Employee in such cases.

2.2 Data Security Incident

A "**Data Security Incident**" is any actual, potential or suspected incident or occurrence involving the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access to Relevant Data.

"**Relevant Data**" is data (information) in any form (whether it is personal data or confidential information or not, and whether stored electronically, in hard copy, or otherwise) that is controlled or processed by Modern Expo or on Modern Expo's behalf directly or indirectly. Relevant Data includes, for example, data that is hosted by a vendor or other service provider at Modern Expo's request.

Relevant Data can be contained, for example, in paper files, emails, spreadsheets, personnel records, payroll records, servers, portable storage devices (such as a laptop, a smartphone or flash drive), or in IT databases.

Below are examples of events which must be immediately reported as a Data Security Incident to **databreach@modern-expo.com**:

- Theft or loss of any paper records or any computer, laptop, smartphone, thumb drive, or other data storage that has ever been used to store data relating to Modern Expo.
- An email inadvertently sent to the wrong recipient(s).
- Unauthorised access to a system or to any Modern Expo premises.
- Behaviour amounting to a breach of the Information Security Policy.
- A break-in or robbery at a Modern Expo facility (actual or attempted).
- An attacker compromising the Company’s databases, computers, networks, communications, etc.
- Employees viewing, accessing or disclosing information, files or databases outside the scope of their assigned responsibilities.
- Breach by a third party of a non-disclosure agreement or confidentiality agreement.
- Any of the above events if they concern a vendor or other service provider of Modern Expo.

2.3 Assistance

Each Employee is required to assist Modern Expo and the Incident Response Team in the investigation of a Data Security Incident.

3. Incident Response Team

The Incident Response Team consists of a member of the highest management of the relevant Modern Expo entity as well as the heads of the following business functions:

- Legal
- IT and Information Security
- Property Security
- Human Resources

The heads of the relevant business functions can designate other persons to take part in the Incident Response Team in their place, by notice to all other members of the Incident Response Team (with a copy to databreach@modern-expo.com).

3.1 Incident Response Team Leader

The Incident Response Team will be led by the member of the highest management of the relevant Modern Expo entity, unless he or she appoints another leader. The leader of the Incident Response Team bears the ultimate responsibility for carrying out the functions assigned by this Policy to the Incident Response Team.

4. Data security incident response procedure

4.1 Conduct Initial Investigation

The preliminary investigation of each reported incident is carried out by a member of the Incident Response Team from the Legal function (the "**First Responder**"), unless another First Responder is designated by the Incident Response Team from time to time.

The First Responder promptly responds to the reporting Employee and obtains as much information as is readily available about the Data Security Incident. If the Data Security Incident involves information technology or other computer security issues, the First Responder coordinates with the IT & Security member. The First Responder should make an initial determination promptly (usually within 24 hours) as to whether, based on available information, a reasonable basis exists to believe that a Data Security Incident has occurred or might have occurred. If no reasonable basis exists, the First Responder completes an internal report that includes the following information:

- the identity of the reporting Employee (or Employees);
- a description of the circumstances of the reported Data Security Incident; and
- an explanation of why the First Responder determined that there was no reasonable basis to believe there have been or might have been a Data Security Incident.

The First Responder promptly provides the written report to the other members of her/his Incident Response Team and sends a copy to databreach@modern-expo.com.

4.2 Notify the Incident Response Team

If the First Responder determines that there is a reasonable basis to believe that a Data Security Incident occurred or might have occurred, the First Responder immediately notifies the other members of the Incident Response Team.

4.3 Determine the Scope of the Data Security Incident and Applicable Legal Requirements

The Incident Response Team takes the following actions as applicable and appropriate under the circumstances:

(a) **Investigate the Scope of the Data Security Incident.** The Incident Response Team investigates and gathers information regarding the scope of the suspected Data Security Incident, including, as appropriate:

- when and how the suspected Data Security Incident occurred and when it was discovered;
- the categories of information (e.g., types of personal data) that may be at risk of compromise;
- the risks of potential abuse or harm; and
- who knows about the suspected Data Security Incident inside and outside of Modern Expo.

(**Appendix B** sets out a potential Data Security Incident checklist that the Incident Response Team may use as an aid in the investigation.)

(b) **Secure and Isolate the Threat.** If a persistent or ongoing threat (e.g., a hacker or virus on Modern Expo's information systems) occurs, the Incident Response Team ensures that appropriate IT & Security personnel determine appropriate actions to take to secure and isolate the threat so that it does not continue to cause harm to Modern Expo's technical environment.

(c) **Preserve Evidence.** In conducting the investigation, the Incident Response Team seeks to ensure that appropriate actions are taken to preserve any relevant information and evidence, including:

- suspending any data deletion or destruction practices (including automated log file or backup tape overwriting or recycling);
- instructing Employees, contractors, agents, or representatives with system access to exercise caution so as not to delete, alter, or corrupt relevant information and evidence;
- preserving any suspicious code or suspected malware; and
- issuing any relevant litigation holds in accordance with Modern Expo's policies.

(d) **Retain Forensic Investigators.** If the suspected Data Security Incident involves possible unauthorized intrusions into information systems, the Incident Response Team should advise whether the relevant Modern Expo entity should retain a qualified forensic investigator to image affected devices, conduct a forensic computer investigation, or provide other services.

(e) **Notice to Law Enforcement.** As part of the investigation, the Incident Response Team advises the relevant Modern Expo entity on whether it is necessary or appropriate to notify law enforcement authorities (e.g., European law enforcement agencies, public prosecutor's office, local police, or other authorities).

(f) **Determine Applicable Requirements.** The Group Legal Office and/or external legal counsel advise the Incident Response Team regarding what data security breach notification laws may apply to the Data Security Incident ("**Data Breach Notice Laws**") and whether the Data Security Incident amounts under the Data Breach Notice Laws to a data security breach that triggers amongst others a duty to provide notifications regarding the Data Security Incident to affected individuals, government authorities/data protection supervisory authorities, consumer reporting agencies, the media, or others.

Appendix C outlines a summary of the requirements of the General Data Protection Regulation (GDPR) in respect of notifying data protection authorities and data subjects. Note, however, that national laws of EU countries may require notification even when it is not required by the GDPR.

In addition, the Group Legal Office and/or external legal counsel advise the Incident Response Team on other requirements beyond Data Breach Notice Laws that may require notification of a Data Security Incident, for example:

- Contractual obligations to business partners or others.
- Privacy policies or other statements in internal or external documents regarding notification.

(g) **Confidentiality**. The Incident Response Team shall work with other departments to ensure every suspected Data Security Incident is kept confidential until a decision regarding notification or disclosure is made and shall also keep the number of Employees who know about the Data Security Incident as limited as possible.

(h) **Documentation Requirement**. Whether or not Data Breach Notice Laws apply to the Data Security Incident, the Initial Response Team shall sufficiently document the Data Security Incident, in particular the legal assessment as to applicability of the Data Breach Notice Laws.

4.4 Notify Individuals, Governmental Authorities and Others

The Incident Response Team determines whether it is necessary to make notifications in accordance with the guidance provided by the Group Legal Office or external legal counsel. If a notice is required, the following apply:

(a) **Contents of Notice, Script for Follow-up Questions**. If a notice is required, the Incident Response Team should work with the Group Legal Office and/or external legal counsel to determine the wording and distribution procedure for notifications. If the Incident Response Team decides to use Modern Expo personnel or retain an external call centre to answer the questions of affected individuals who may have questions about the Data Security Incident or related matters, the Incident Response Team develops a script for call centre personnel or other designated contacts who are prepared to accept calls from any affected individuals.

(b) **Form of Notice.** Unless another form of notice is required by applicable law, notification to affected individuals who have provided email addresses to Modern Expo will be made via email with a return receipt requested to any affected individuals. For those who have provided a postal address to Modern Expo, but not an email address, the notice will go out via postal mail. The Incident Response Team works with Group Legal Office and/or external legal counsel to determine the appropriate format for transmitting the notice taking into account applicable law and costs. Other public means of notice (e.g., via a website or state-wide media) are not required by this Policy, but may be required by Data Breach Notice Laws or deemed helpful for customer relations or other purposes in certain situations. If the notice cannot be made in accordance with this Section, the Incident Response Team should immediately consult with the Group Legal Office and/or external legal counsel to determine how to provide substitute notice. The Incident Response Team may delay the transmission of the notice if a law enforcement agency determines that a notice to affected individuals would impede a criminal investigation.

4.5 Keep Records

The Incident Response Team is responsible for the creation and preservation of written records of each Data Security Incident.

Each record must include:

- the facts established in relation to the Data Security Incident

- the assessment of its effects and risks
- the remedial action taken.

The Group Legal Office keeps registers of Data Security Incidents involving a personal data breach for each Modern Expo entity.

4.6 Respond to Inquiries

The Incident Response Team plans how Modern Expo should respond if it receives an inquiry by the press, the government, or any other party.

4.7 Review Insurance Obligations

The Incident Response Team reviews applicable Modern Expo insurance policies to determine if notice should be made in accordance with the provisions of any such policy.

4.8 Remedial Action and Corrective Measures

The Incident Response Team will work with the Group Legal Office and the IT and Information Security Office to determine what technical and organizational security measures are necessary to prevent similar Data Security Incidents in the future, including policies, awareness training, and procedures for Employees. The Incident Response Team will evaluate third-party relationships that might have been involved in the Data Security Incident and recommends appropriate action, e.g., contractual changes, alterations in procedures and/or training, improvements in security measures, changing a vendor, etc.

The Incident Response Team will make recommendations in respect of any changes in internal procedures and processes that are considered desirable in view of the Data Security Incident.

.

Appendix A - Security Incident Reporting Form

Description of the Data Security Incident:	
Time and Date Data Security Incident was identified and by whom.	
Reporting Employee	Name: Position: Department: Company: Country: Email Address: Phone Number:
Affected Systems	
Affected Categories of Individuals (e.g., customers, business partners, employees)	
Affected Categories of Data	
Who has been informed of the Data Security Incident?	

Please send the completed form to **databreach@modern-expo.com**.

Appendix B - Initial Assessment Checklist for the Incident Response Team

- ☐ **What is known about nature of the Data Security Incident?** How did the Data Security Incident come to the attention of the Incident Response Team?
- ☐ **What is known about the nature of the data affected?** Do the affected data fields include any data that could trigger breach notification or other mandatory legal or contractual duties?
- ☐ **What types of individuals may be affected** (e.g., employees, customers, other)?
- ☐ **Where are such potentially affected individuals located** (e.g., EU/EEA only, and if so, what member states, and any non-EU/EEA locations)?
- ☐ **What is the approximate number of affected individuals:** (i) per EU/EEA state; and (ii) per non-EU/EEA jurisdiction?
- ☐ **What is the type and approximate number of affected personal data records?**
- ☐ **What is known about the scope of the Data Security Incident?** If the Data Security Incident may have involved an unauthorized intrusion to information systems, what host machines may have been accessed, what data resides on those machines, and how did the intruders gain access?
- ☐ **What parties are aware of the situation, both internally and externally?**
- ☐ **What steps are being taken to protect the security of the system while avoiding destruction of electronic evidence**?
- ☐ **Has a forensics firm been engaged to perform the tasks described above?** Who is managing the technical and security aspects of the Data Security Incident?
- ☐ **Are appropriate personnel within the company aware of the Data Security Incident** (e.g., senior management, IT, department leads, Human Resources, External Relations, etc.)?
- ☐ **Are there any other key known concerns at this stage?**
- ☐ **Has law enforcement been contacted?** If so, what agency and by whom?

Appendix C - Data Security Incident Notification under the GDPR

1 Has there been a Data Security Incident in respect of personal data?

"**Personal data**" is any information that relates to an identified or identifiable individual.

If **yes**, go to 2. If **no**, the GDPR reporting obligation does not apply.

2 Is Modern Expo a controller or processor of the personal data?

If Modern Expo is a **processor**, it must notify the controller of the personal data about the breach without delay. (Modern Expo is a processor if it processes personal data on behalf of the controller).

If Modern Expo is a **controller**, go to 3. (A controller is the person who determines the purposes and means of the processing of personal data, alone or jointly with some other person(s)).

If Modern Expo is **neither**, the GDPR reporting obligation does not apply to it.

3 Is the breach likely to result in a risk to the rights and freedoms of individuals?

For example, can the breach lead to physical, material or non-material damage to the individuals whose data have been breached, loss of control over their personal data, limitation of their rights, discrimination, identity theft, fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage?

If **yes**, go to 4. If **no**, the GDPR reporting obligation does not apply. However, the breach must be registered and all relevant records kept.

4 Notify the competent data protection authority

4.1 By when?

Notify without delay, where feasible not later than 72 hours after having become aware of the breach. If not made within 72 hours, the notification must be accompanied with explanation of the reasons for the delay.

4.2 Where?

Notify the data protection authority in the state where the controller of the personal data is located. See **Appendix D** for contact details of the relevant authorities.

In cases of doubt, seek advice or consider the guidance in the WP29 Guidelines on the Lead Supervisory Authority (wp244rev.01): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

After the United Kingdom exits the European Union, notification of the UK authority may not be sufficient even if the controller of the relevant data is Modern Expo's UK entity. If the breach relates to personal data of individuals in an EU state, the competent authority of that state should also be consulted and/or notified.

4.3 What to notify?

The notification must at least:

- identify the controller of the personal data;
- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer (if the controller has formally designated one) or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5 Consider notifying the individuals concerned

5.1 Is it necessary?

Notification of each individual is mandatory if the breach is likely to result in a high risk to the rights and freedoms of the individuals, except where one of the following cases apply:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individuals is no longer likely to materialise;
- personal notification would involve disproportionate effort. In such a case, there must instead be a public communication or similar measure whereby the individuals are informed in an equally effective manner.

In cases of doubt as to whether the breach is likely to result in a high risk, seek advice or consider the guidance in the WP29 Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679 (wp248rev.01): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

5.2 What to notify?

The notification must describe in a clear and plain language the nature of the breach, and contain the same information that is required to be given to the data protection authority (see 4.3 above).

5.3 By when?

The notification must be made without delay.

6 Consider notification requirements under national law

National laws of EU countries may require notification of data subjects and/or data protection authorities even when this is not required by the GDPR.

Appendix D - Contacts of Data Protection Authorities (data breach notifications)

1. France

Language: French

Form of the data breach report (submitted online): https://notifications.cnil.fr/notifications/index

More information: https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

2. Germany (Berlin)

Language: German

Form of the data breach report:
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/datenleck/BlnBDI_formular_datenpanne.pdf

Completion tips: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/datenleck/BlnBDI_formular_datenpanne_hinweise.pdf

Postal address:

Berlin Commissioner for Data Protection and Freedom of Information
Official Data Protection Officer
Friedrichstr. 219
10969 Berlin

Email address: behDSB@datenschutz-berlin.de

Telephone: +49 30 13889-406

3. The Netherlands

Language: Dutch

Form of the data breach report (submitted online):
https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1

Postal address:

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ DEN HAAG

Telephone numbers:
+31 - 88 - 1805 255
+31 - 70 - 888 85 00
Fax: +31- 70 - 888 85 01

4. Poland

Language: Polish

Form of the data breach report (submitted online): https://www.biznes.gov.pl/pl/firma/sprzedaz-i-marketing/chce-sprzedawac-przez-internet/proc_889-naruszenie-danych-osobowych

Additional information: https://uodo.gov.pl/pl/134/233

Postal address:

Urząd Ochrony Danych Osobowych
Stawki 2, 00-193 Warsaw

Telephone: +48 22 531 03 00

5. United Kingdom

Language: English

Form of the data breach report: https://ico.org.uk/media/for-organisations/documents/2614197/personal-data-breach-report-form-web-20190124.doc

Postal address:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
United Kingdom

Electronic address:
Email the report to casework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Telephone: +44 303 123 1113