**Data Breach Incident Response Manual
[COMPANY]**

[***Note: This template details a complete step-by-step checklist how personal data breaches need to be escalated in a timely manner. Use this template in response to a personal data breach***]

# SCOPE

The purpose of this Data Breach Incident Response Manual (the "**Manual**") is to provide you with concrete information on how to identify and deal with security incidents involving loss of personal data. Loss of personal data may constitute a breach of data protection laws and/or require notification to local data protection supervisory authorities.

All employees, consultants, suppliers and contractors of [Company] (“[**Company**]”), to whom this Manual or a part of it is applicable (“**Stakeholders**”) are required to comply with the Manual.

The Manual consists of the following key chapters:

1. **Checklist** - A step-by-step guide that the Stakeholders and the Breach Response Team need to follow in case of a data breach.
2. **Schedules** - A set of useful documents to illustrate and supplement the Policy and Checklist, including:
	* **Schedule 1**: a template form to **log security incidents** in view of documenting data breaches within [Company] in a systematic and consistent manner;
	* **Schedule 2**: a description of the methodology for the **assessment of risk**;
	* **Schedule 3**: a **template communication** towards the affected data subjects or a notification to the regulators in relation to the occurrence of a data breach.

# POLICY

* 1. **Detecting and responding to a data breach**

We have a four-step approach to dealing with data breaches involving detection, assessment, response handling and review. Each of these steps are explained in in section 3 ("Checklist").



This Manual serves as a **preparation** for all Stakeholders in anticipation of a data breach. While not all data breaches may be avoided, our company can plan for it and significantly reduce the impact that a data breach has on our organization, both financially and in terms of reputation. It is therefore crucial that you familiarize yourself with this Manual.

Apart from overall preparation, there are four other steps to be taken in relation to handling a data breach. For each of those 4 steps, we have created a practical checklist for detecting, assessing, responding to, reporting and reviewing a data breach.

* 1. **Checklist for all Stakeholders (Step 1)**

**Step 1 - Detection**

We expect data breaches to be notified through three main channels:

* **Employee reporting** - All employees and other Stakeholders are encouraged to report a potential data breach or concerns relating to a data breach to the [to be completed by [Company]], even if there is only a serious suspicion and no concrete evidence at that stage.

We encourage openness amongst staff to report actual or suspected data breaches and will not take disciplinary action against members of staff who may have been involved in a data breach, provided they report the breach in accordance with this Manual and where their involvement in the breach was not deliberate.

* **Monitoring by** [**IT department / external IT service provider**]- Our [IT team / IT service provider] routinely monitors our IT and other operating systems to detect potential security incidents and data breaches. While most minor incidences will be dealt with directly by the [IT team / IT service provider] (for example minor breaches of acceptable use policies etc.), more serious incident are expected to be escalated to the [the head of the [IT team / IT service provider]], who subsequently will be tasked with notifying the [Privacy Officer/Compliance Manager] as appropriate.
* **Third party / external notifications** - If a third party (e.g. a customer or supplier representative) becomes aware of an actual or potential security incident or data breach, it is important that any notification provided to us is properly captured and assessed. Additionally third parties that process on behalf of [Company] should be contractually obliged to notify a data breach to us. All third parties will be instructed to report any incident or data breach to [Privacy Officer/Compliance Manager].

Employees are expected to be proactive in escalating any information provided by third parties about a potential data breaches to the [Privacy Officer/Compliance Manager].

When you become aware of an incident that in your belief may constitute a data breach, you are required to follow the following steps. Please note that depending on the concrete circumstances, the relevance of the chronology set forth below may change.

|  |
| --- |
| **STEP 1 - DETECTION** |
| **N°** | **Action** | **Owner** |
| 1 | Escalate the incident to the [Privacy Officer/Compliance Manager]. Contact details of the [Privacy Officer/Compliance Manager] can be found in [Schedule 2] of this Manual. | All Stakeholders |
| 2 | When the [IT team / IT service provider] becomes aware of a data breach, they will also notify the [Privacy Officer/Compliance Manager]. |
| 3 | Where required and upon request, assist the [Privacy Officer/Compliance Manager] to the best of your ability.  |
| 4 | Maintain any relevant documentation that may assist with logging the incident afterwards. Please refer to the template form in Schedule 1 of this Manual to learn more about the information typically required to log an incident. |
| 5 | Do not communicate about the breach to others in your team who do not have a strict need-to-know, nor to any persons outside [Company]. |
| 6 | Do not probe computers and affected systems without IT approval. |
| 7 | Do not turn off computers and affected systems without IT approval. |
| 8 | Do not image or copy data, or connect storage devices/media to affected systems. |
| 9 | Do not run anti-virus programs or utilities without IT approval. |
| 10 | Do not reconnect affected systems without IT approval. |

**Step 2- Assessment**

Following detection of a (potential) data breach , the [Privacy Officer/Compliance Manager] - notified by an employee, the [IT team / IT service provider] or a third party - will further lead the incident response procedure. For this phase, the following steps are to be followed, whether or not in chronological order, depending on the concrete circumstances:

|  |
| --- |
| **STEP 2 - ASSESSMENT**  |
| **N°** | **Action** | **Owner** |
| 1 | Instruct the [IT team / IT service provider]/Head of the [IT team / IT service provider] to manage the initial technical assessment of the potential data breach. | [Privacy Officer/Compliance Manager] |
| 2 | Instruct the [IT Team / IT service provider] in case of a breach to carry out a technical assessment of the severity of the breach, including the nature of information accessed and the extent of access.  | [Head of the IT Team / IT service provider] |
| 3 | Grant relevant access permissions to members of [IT team / IT service provider] where required. | [Head of the IT Team / IT service provider] |
| 4 | Communicate findings of the technical assessment to the [Privacy Officer/Compliance Manager]. | [Head of the IT Team / IT service provider] |
| 5 | Request additional investigation by the [IT team / IT service provider] of the data breach where required. | [Privacy Officer/Compliance Manager] |

**Step 3 - Response**

Once the initial technical assessment of the data breach was carried out, the incident should be responded to in a manner appropriate to its characteristics and the circumstances surrounding the incident.

Based on the findings of the technical assessment, the [to be completed by [Company]] will coordinate the response, and will report upon regular intervals to the [to be completed by [Company]], as agreed with the latter.

If, based on the nature of the breach, it appears that email systems of [Company] may be compromised, it should be considered to communicate by telephone to prevent vital communications from leaking.

| **STEP 3 - RESPONSE**  |
| --- |
| **N°** | **Overall action** | **Specific action steps** | **Owner** |
| 1 | **Internal review** - Establish a breach response team and organise a meeting where you deliberate and discuss the facts known to date, including the nature of information accessed and extent of the access.This typically includes details on who was involved, what happened, where it happened, when it happened, how it happened and how [Company] can remediate the breach.The discussions are to be based on the initial technical assessment provided by the [Head of the [IT team / IT service provider]]. | 1. Contact outside counsel to understand legal implications of the breach and confirm a legal strategy.
2. Establish a privileged breach response team portal to memorialize actions taken to provide legal advice and direction.
3. Draft (preliminary outline of) breach response strategy, including any actions to be taken and ownership for each action.
 | a) [Head of the [IT team / IT service provider]]b) [Privacy Officer/Compliance Manager] c) other Stakeholders depending on the circumstances of the data breach |
| 2 | **Investigation** - The team must assess whether the information and findings gathered so far in relation to the breach are sufficient to understand the nature of the incident, the impact on the organisation (in terms of legal liability, reputational damage, financial impact, organisational impact and other risk factors), and help establish the underlying cause and impacted stakeholders. | 1. Brief the team about containment, status of investigation, and other relevant aspects.
2. Assess completeness and accurateness of information gathered so far.
3. Where required: order additional investigation from [IT team / IT service provider] staff, external cybersecurity and/or forensic experts.
4. Determine how to address the breach while ensuring or restoring business continuity.
5. Identify the individuals who were involved in the discovery and initial investigation of the breach. Document their actions and findings, and organise interviews with these persons, as necessary, to obtain any missing information.
6. Taking into account the status of the investigation, consider notifying the the Executive Committee and Board of Directors, as appropriate [OPTIONAL].
 | a) [Head of the [IT team / IT service provider]][By retaining external experts, communications prepared for or by the external experts can be protected by the attorney-client privilege.]b) [Privacy Officer/Compliance Manager] c) other Stakeholders depending on the circumstances of the data breach |
| 3 | **Containment** - Agree on steps to be taken to contain the breach to prevent any further data loss or security compromises.  | 1. If the breach is ongoing, consult with forensic experts [and trained [Information Security] staff] about taking affected systems offline by disconnecting them from the network, and/or using tools to dynamically image affected systems to preserve evidence.
2. Where the breach does not concern personal data of employees, consider notifying employees about the breach, to ensure appropriate actions are taken to contain the breach at individual level.
3. Change security access devices and passwords where required.
4. If the breach involves breach of payment card date, obtain legal guidance on additional steps that need to be taken, and obtain a list of affected credit card numbers as soon as possible.
5. Determine any legal implications of indemnification and/or responsibility of third parties, if a third party is the cause of the breach.
 | a) [Head of the [IT team / IT service provider]][By retaining external experts via Legal, communications prepared for or by the external experts can be protected by the attorney-client privilege.]b) [Privacy Officer/Compliance Manager] c) other Stakeholders depending on the circumstances of the data breach |
| 4 | **Restoration** - Restoring any services impacted by the breach as soon as possible once the breach has been contained. | This may include recovering data from suitable backup systems, provided all traces of the compromise have been removed. | [Head of the [IT team / IT service provider]] |
| 5 | **Intervention and improvement** - Apply intervention and improvement processes to existing business processes to prevent recurrence of the incident.  | This may be supported by targeted security awareness training or legal action. | [to be completed by [Company]] |
| 6 | **Preservation of evidence** - If it is decided to pursue a perpetrator of the data breach it will be essential to take a forensic copy of the affected system immediately after the security breach was detected as evidence of the breach. | 1. Consult with cybersecurity and forensic experts before 'touching' data potentially at issue.
2. Preserve all affected system log files, including firewall, VPN, mail, network, client, web, server and intrusion detection system logs.
 | a) [Head of the [IT team / IT service provider]]b) [Privacy Officer/Compliance Manager]  |
| 7 | **Documentation -** Maintain adequate documentation of the data breach. System logs are critical to assessing the origins of the attack, its duration, and volume of data affected during the breach. This information can help contribute to establish 'lessons learned'. | 1. Record the date and time of the breach, the personnel who discovered the breach, the nature of the breach, the kinds of data stolen/lost, when the response efforts began and all of the employees who had access to the affected systems. Cf. Schedule 1 for a template log form.
2. Confirm that the security access has been terminated for any employee suspected to have been deliberately involved in the breach.
 | a) [Head of the [IT team / IT service provider]] |
| 8 | **Engagement with stakeholders (notification)** - It is important to effectively engage with those directly affected by the breach, or those who may have a wider interest in management of the breach. This is likely to include employees, the media, clients and appropriate regulators or law enforcement agencies. An engagement plan should be agreed at the earliest opportunity.Please note that depending on the particular circumstances and on the legal advice gained from local outside counsel, **it may be legally required to notify the persons affected, law enforcement and/or regulators at an earlier stage and more specifically within 72 hours for data breaches affecting European entities.**Please refer to the table below for more information. | 1. Consult table below for specific notification actions in relation to each category of individual or authority concerned.
2. Determine who has responsibility for notification ([Company], or a client or vendor).
3. Develop engagement / communications plan.
 | a) [Head of the affected departments]b) [Privacy Officer/Compliance Manager] c) other Stakeholders depending on the circumstances of the data breach (e.g. in this case Legal department, Human Resources.) |
| 9 | Continue convening team meetings, as required. | Continue reviewing breach response strategy and progress on actions list. | Breach response team |
| 10 | Continue updating the Executive Committee and Board of Directors, as appropriate. | N/A | [Privacy Officer/Compliance Manager]  |

**Notification and engagement with stakeholders**

In relation to notification, guidance from [the Legal department / external legal counsel] must be sought before engaging with staff or any external stakeholders to ensure information disclosed is accurate and does not expose us to undue risk. The [the Legal department / external legal counsel] will determine whether and how to notify data breaches, as notification requirements vary country-by-country and inappropriate action may result in enforcement action.

The table below provides an overview of best practices in relation to notifying the stakeholders. Notification of, or engagement with these stakeholders should take place in strict compliance with the engagement plan developed by the breach response team, and only by those persons explicitly authorised for such engagement. With the exception of personnel, we should carefully evaluate when to notify or communicate to the affected individuals, other third parties and authorities when this is not legally or contractually required.

| **NOTIFICATION - ENGAGEMENT WITH STAKEHOLDERS** |
| --- |
| **Stakeholder** | **Action** |
| Personnel  | * Inform personnel of appropriate information in a timely manner to limit rumours.
* When there is a high risk to the rights and freedoms of the personnel, you may be obliged to communicate the personal data breach to the personnel without undue delay.
* Originate communications from a trusted source with indications of timing for updates.
* Provide "do not forward" instructions on all incident-related communications.
 |
| Clients, B2B customer or other data subjects | * When there is a high risk to the rights and freedoms of these data subjects, you may be obliged to communicate the personal data breach (provide with clear and detailed notification letters) to these data subjects within undue delay.
* Provide contact information for clients and/or users to seek additional information.
* Provide information on the type of data that may have been exposed, potential impact on clients and/or users, and [Company]’s response.
* [OPTIONAL] Partner with [Public Relations and Legal] teams to create notification letters in accordance with applicable laws and regulations.
 |
| [OPTIONAL] Media | * Work with the [Public Relations] department to handle interactions with the media and to develop a timely incident communication strategy.
* Prepare a preapproved proactive statement to be released where appropriate with clear 'lines to take'.
* Create a specific e-mail inbox to facilitate communications with the media.
* Consider relevant legal, ethical, and reputational ramifications during press releases.
 |
| Authorities and regulators | * Be clear when there is a legal requirement to notify a regulator (e.g. data protection supervisory authorities) or law enforcement body about a breach.
* When there is a high risk to the rights and freedoms of any data subject, you may be obliged to notify the data subject(s) concerned.
* Consider involving a regulator or law enforcement agency voluntarily about a breach voluntarily (e.g. if you suspect foul play), as they may help with establishing next steps to manage the breach, based on their experience with similar incidents.
 |

**Step 4 - Reporting & Review**

|  |
| --- |
| **STEP 4 - REPORTING & REVIEW**  |
| **N°** | **Overall action** | **Specific action steps** | **Owner** |
| 1 | Continue monitoring compliance with legal obligations. | E.g. ensure that any necessary breach notifications have been made. | [to be completed by [Company]] |
| 2 | Monitor internal response to the breach and assess whether further communication with employees is required. | If required, develop and send additional communications to employees. | [Privacy Officer/Compliance Manager / HR] |
| 3 | Monitor external response to the breach and assess whether further external communication with the public and/or media are required. | 1. If required, develop and send additional communications to the general public and/or media.
2. Assess whether persons affected by the breach require additional information. If required, develop and send additional communications to the affected persons.
 | [Privacy Officer/Compliance Manager] |
| 4 | Conclude ongoing investigations once it is found that the incident is resolved. | N/A | Breach response team |
| 5 | Based on the log form(s) of the breach, produce an Incident Report [OPTIONAL: for [Company]’s Executive Committee and Board of Directors, as appropriate]. | The Incident Report should include the following:* A summary of the breach (date, description, division(s) and staff involved);
* Extent of regions/countries potentially affected;
* Who has been notified;
* Actions taken with dates and action owners;
* Estimate of the financial cost and business impact of the incident;
* Recommendations for changes to avoid future occurrences;
* Estimated timescale for the implementation of recommended changes pending management authorization.
 | Breach response team(Outside counsel)(External experts) |
| 6 | Notify all parties and stakeholders involved that the incident is resolved. | 1. Prepare the communications.
2. Coordinate the notification.
 | Breach response team |
| 7 | Convene a post-breach meeting of the breach response team. | The meeting should cover the following issues:* Did the detection and response procedure work as intended?
* If not, in what areas is improvement required?
* What changes could be made to procedures to improve our ability to detect and handle similar incidents?
* What tools worked well and what additional tools would be useful in the future?
* Was the level of the response appropriate?
* Could any lessons be learnt from the incident?
 | Breach response team |
| 8 | Add output of the post-incident review meeting to the Incident Report. | N/A | Breach response team |
| 9 | Review operational controls and update as necessary. | This may include revising data collection controls, training, etc. | [Head of the [IT team / IT service provider]] |
| 10 | Review training of all personnel, including [IT team / IT service provider], and update as necessary. | Remind the appropriate parties that potential concerns about incidents must be notified to the [Privacy Officer/Compliance Manager]. | [Privacy Officer/Compliance Manager] / HR |

* 1. **Review and updates**

All updates in response to applicable regulations, internal operational procedures or other requirements shall be made promptly by the [Privacy Officer/Compliance Manager], who will review and obtain approval from the breach response team for all updates to this Manual within a reasonable timeframe.

For questions about this Manual, contact [Privacy Officer/Compliance Manager] at [insert contact details].

##### SCHEDULE 1 – fORM FOR loGGING DATA BREACH

| **(Potential) Incident Log** |
| --- |
| **Information** | **Description** |
| Unique identifier | *[Insert name / log code convention to distinguish data breaches]* |
| Owner of the incident | *[List of current and historical owners of the data breach, including contact information for individuals]* |
| Description of the incident | *[Insert overview of the data breach, including searchable key words and include Users affected and systems affected]* |
| Summary of action steps | *[Insert a description of the steps taken to contain and recover from the data breach]* |
| Dates and times for all events | *[Set out a list / details of the times for occurrence, discovery, containment, and recovery]* |
| Identification of the incident | *[Detail the method of identification of the data breach]* |
| Severity level | *[Detail the impact of the data breach]* |
| Required staff effort to remediate incident | *[Set out a quantification of staff hours required to contain / recover / deal with from the data breach]* |
| System downtime | *[Where applicable include details of the number of hours a system was unavailable to the business]* |
| Resolution | *[Describe how the data breach was resolved]* |
| Preventable incident | *[YES / NO]* |
| Other relevant information | *[Detail any other information that you may deem relevant in relation to the data breach.]* |

##### SCHEDULE 2 – Assessment of the risk

When there are no likely adverse effects on individuals, no notification to the data subjects and the supervisory authority is necessary. Hence this evaluation is an important one that should be documented. In order to asses these adverse effects and to categorize the data breach as a high or critical severity it is necessary to take into account all the appropriate elements.

Please note that the following criteria only **serve as guidance** and should be amended in accordance to the specifics of [your company]. Further the criteria should be assessed together and one has no priority over the other.

1. Number of data subjects affected

In principle the number of data subjects concerned is **not a determining factor** and the notification should depending on the likely adversely effects, independently to the number of data subjects concerned.

However if the contact details of one person are accidently disclosed by forwarding an email to a third party, it is seemingly not worth to go through the internal and external administration process. If the contact details of all employees of a multinational or the details of all consumers would be disclosed, it would be suggested to notify.

There is no benchmark on this matter and it should be recommended to notify within doubt.

1. The type of personal data

The type of personal data is an **essential and determining** factor in the assessment. The sensitivity of the personal data may require the notification of a data breach relating to one single individual.

Generally sensitive personal data would require a notification (a person’s religion or beliefs, race, political opinion, health, sexual life, trade Union membership, as well as criminal personal data).

It also includes data which would allow stigmatization or exclusion of the data subject, damage the health, financial damage or (identity) fraud or data relating to the financial or economic situation of the data subject. It may also include user names, passwords and other login data.

1. The applied technological protection and organisational measures applied to the personal data

The applied technological protection and organizational measures is another **essential and determining** factor in the assessment. Since a notification to data subjects or communication to the supervisory authority is required when the breach does not adversely affect the personal data or privacy of the data subjects. Depending on the applied measures, no risk for the data subjects can be involved.

Although these measures needs to be **evaluated on a case-by-case basis to assess if they have limited the risk for the data subject**, guidance from the WP29 has allowed to list examples of what these measures could be.

1. The potential to incur large financial risks or legal liability for the company

Although from the authorities perspective, the data subject should be central in this assessment, from your organizations perspective it is essential to also take into account the financial risks and legal liability you may incur. We suggest to approach your notification and communications duty as the best-in-class where you risk large financial or legal liability which takes into account the public relations impact.

##### SCHEDULE 3 – TEMPLATE COMMUNICATIONS/notifications

1. **Employee or other data subject communication**

Depending on the circumstances, this letter **should be tailored to the factual differences and legal differences** A breach affecting employee data or data of other data subjects (e.g. consumers, identifiable individuals from third parties) only requires a notification depending on the high risk for the rights and freedoms of the data subject and the conditions that [Company] has implemented to secure the personal data affected. [INSERT PERSON] will evaluate the need to notify the data subject [and inform the [INSERT PERSON] to amend the notice below depending on the circumstances described by [REINSERT PERSON] to [INSERT PERSON].

**Notice of Data Breach**

Dear \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

As a valued employee/consumer/other data subject of [Company] International (“[Company]”), we are writing to inform you about a security incident that affected your personal data. We take the security of your personal data seriously and we sincerely regret the effect this incident may have had on you. Please read this letter for more information about the incident, the services we’re offering to you in response and steps you can take.

**What Happened?**

On [DATE], [Company] was the victim of [SPECIFY THE CAUSE - e.g. an email phishing incident, one of our employees, acting in good faith, shared sensitive information with an outside party posing as a [Company] executive] that resulted in [SPECIFY THE RESULT - e.g. an unauthorized disclosure of your personal data to third parties].

**What Personal Data Was Involved?**

The personal data involved in this incident includes [INSERT PERSONAL DATA DISCLOSED – e.g., your name, address, Social Security number, income information, and …]. At this time, we have no reason to believe any other personal data was affected.

**What Are The Possible Consequences ?**

Due to the [REINSERT THE RESULT], your personal data involved in this incident may be exposed to [SPECIFY POSSIBLE CONSEQUENCES].

**What Are We Doing?**

We learned of the incident on [DATE] and promptly initiated our Data Breach Incident Response procedure with an investigation into what happened, [engaged third party forensic experts] and reported it to [INSERT ANY LAW ENFORCEMENT AND/OR CREDIT BUREAUS].

In addition, we [INSERT OTHER STEPS [Company] IS TAKING IN RESPONSE TO THE INCIDENT].

We take the security of your personal data seriously and sincerely apologize to anyone who may have been affected. To assist you in protecting your personal data against [INSERT POSSIBLE RESULT], we are offering the following services:

* [INSERT POSSIBLE SERVICE TO REMEDY THE RESULT]. This […] helps to [ INSERT WHAT THE SERVICE WILL DO - e.g. detect possible misuse of your personal data and provides you with identity protection support focused on immediate identification and resolution of potential identity theft and HOW they can request the service.]
* [INSERT POSSIBLE SERVICE TO REMEDY THE RESULT]. This […] helps to [ INSERT WHAT THE SERVICE WILL DO and HOW they can request the service]
* [INSERT POSSIBLE SERVICE TO REMEDY THE RESULT]. This […] helps to [ INSERT WHAT THE SERVICE WILL DO and HOW they can request the service]

**What You Can Do.**

In addition our proposed services, we recommend that you:

* [INSERT RECOMMENDATION].
* [INSERT RECOMMENDATION].
* practice good data security by ensuring that your computer has anti-virus protection and that it is up-to-date and by updating your passwords regularly and ensuring that your passwords are complex and unique
* pay particular attention to any emails asking for personal data, financial information, or SSNs. Please do not give out your Social Security number or other personal data to unknown sources.
* remain always alert to phishing scams. Phishing scams involve fraudulent (i.e., fake or “spoofed”) email messages that appear to come from legitimate sources and encourage you to (i) click on a link or open an attachment that will download malware onto your computer, or (ii) provide an unknown third party with certain types of information. For example, you may receive an email that directs you to input information, such as your user name and password, into an unauthorized website like [WEBSITE] You may also receive an email from a source that appears to be legitimate but may be off in some way. An email may also be a phishing scam if it has certain anomalies, such as misspellings or awkward phrasing.

Please always forward any suspicious emails to [INSERT IT SECURITY’S EMAIL ADDRESS] before you click on any links, open any attachments, or respond in any way.

**For More Information.**

We sincerely regret that this incident occurred and will continue to [REITERATE A STEP BEING TAKEN IN RESPONSE TO INCIDENT] to ensure that a similar incident never happens again at [Company]

If you have any questions, please feel free to contact [INSERT TITLE AND ROLE OF THE PERSON RESPONSIBLE FOR THE FUNCTION OF A DATA PROTECTION OFFICER OR CHIEF PRIVACY OFFICER] for more information on this matter:

Email: [INSERT]

Phone: [INSERT]

Address: [INSERT]

Sincerely,

[INSERT NAME]

[INSERT TITLE]

1. **Notification to the data protection authority**

Several data protection authorities have online notification forms to report a data breach, hence this form would not be necessary. Additionally the represented guidance here below for such a notification is based on the data protection legislation applicable to the Member States of the European Union, namely the General Data Protection Regulation (“GDPR”).

The template of the notification to the supervisory authority should include at least the following:

(a) 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;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained (e.g. it would be suggested to include here the compliance manager);

(c) describe the likely consequences of the personal data breach;

(d) 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.