Data Breach Policy

Introduction

This Policy aims to help the Law Firm manage personal data breaches effectively. Law Firm holds Personal Data about our employees, clients, users, suppliers and other individuals for a variety of business purposes.

A data breach generally refers to the unauthorized access and retrieval of information that may include corporate and / or personal data. Data breaches are generally recognized as one of the more costly security failures of organizations. They could lead to financial losses, and cause consumers to lose trust in Law Firm .

The GDPR regulations across the various jurisdictions in which Law Firm operates require Law Firm to make reasonable security arrangements to protect the personal data that we possess or control, to prevent unauthorized access, collection, use, disclosure, or similar risks.

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

As our Data Protection Officer, Elena Christodoulou has overall responsibility for the day-to-day implementation of this policy.

Training

All staff will receive training on this policy. New staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the law or our policy and procedure.
Training is provided through an in-house seminar and online training on an annual basis, and covers the applicable laws relating to data protection, and Law Firm ' data protection and related policies and procedures.
Completion of training is compulsory.
If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Applicable Legislation Considerations

http://www.dataprotection.gov.cy

EU GENERAL DATA PROTECTION REGULATION (EU) 2016/679 (GDPR)

Regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents.

Personal Data

Law Firm defines Personal Data as the broader of the definitions contained in the GDPR.
Law Firm defines Sensitive Personal Data as the broader of the definitions contained in the GDPR.
Any use of sensitive Personal Data is to be strictly controlled in accordance with this policy.
While some data will always relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute Personal Data unless it is associated with, or made to relate to, a particular individual.

Generic information that does not relate to a particular individual may also form part of an individual's Personal Data when combined with Personal Data or other information to enable an individual to be identified.

Law Firm gathers Personal Data for two purposes, to identify and protect the data given to us by our customers, and for internal operations.

Personal Data relates to identifiable individual users and may include:
User profile information such as Full name, Photograph, Date of Birth, Mobile telephone number, and Personal email address;

Personal Data we gather for internal operational purposes relates to identifiable individuals such as job applicants, current and former employees, contract and other staff, clients, suppliers, and marketing contacts, and the data gathered may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Causes
Data breaches may be caused by employees, parties external to the organization, or computer system errors.

Human Error
Human Error causes include:
Loss of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
Disclosing data to a wrong recipient
Handling data in an unauthorized way (eg: downloading a local copy of personal data)
Unauthorized access or disclosure of personal data by employees (eg: sharing a login)
Improper disposal of personal data (eg: hard disk, storage media, or paper documents containing personal data sold or discarded before data is properly deleted)

Malicious Activities
Malicious causes include:
Hacking incidents / Illegal access to databases containing personal data
Hacking to access unauthorized data via the Coaching App or API
Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
Scams that trick Law Firm staff into releasing personal data of individuals

Computer System Error
Computer System Error causes include:
Errors or bugs in Law Firm ' Application
Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems

Reporting Breaches
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:
Investigate the failure and take remedial steps if necessary
Maintain a register of compliance failures
Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures

Under the GDPR, the DPO is legally obliged to notify the Supervisory Authority within 72 hours of the data breach (Article 33). Individuals have to be notified if adverse impact is determined (Article 34). In addition, Law Firm must notify any affected clients without undue delay after becoming aware of a personal data breach (Article 33).

However, Law Firm does not have to notify the data subjects if anonymized data is breached. Specifically, the notice to data subjects is not required if the data controller has implemented pseudo-anonymisation techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach (Article 34).

Data Breach Team

The Data Breach Team consists of the CEO with our Data Protection Officer. DPO has the responsibility to make all time-critical decisions on steps taken to contain and manage the incident.

The Data Breach Team should immediately be alerted of any confirmed or suspected data breach via email:

Dataprotection@egc-lawyers.com

The notification should include the following information, where available:

Extent of the data breach

Type and volume of personal data involved

Cause or suspected cause of the breach

Whether the breach has been rectified

Measures and processes that the organization had put in place at the time of the breach

Information on whether affected individuals of the data breach were notified and if not, when the organization intends to do so

Contact details of Law Firm staff with whom the supervisory authority can liaise for further information or clarification

Dataprotection@egc-lawyers.com

info@egc-lawyers.com

Where specific information of the data breach is not yet available, Law Firm should send an interim notification comprising a brief description of the incident.

Notifications made by organizations or the lack of notification, as well as whether organizations have adequate recovery procedures in place, will affect supervising authorities' decision(s) on whether an organization has reasonably protected the personal data under its control or possession.

Responding to a Data Breach

DATA BREACH MANAGEMENT PLAN

Upon being notified of a (suspected or confirmed) data breach, the Data Breach Team should immediately activate the data breach & response plan.

Law Firm ' data breach management and response plan is:

Confirm the Breach

Contain the Breach

Assess Risks and Impact

Report the Incident

Evaluate the Response & Recovery to Prevent Future Breaches

CONFIRM THE BREACH

The Data Breach Team (DBT) should act as soon as it is aware of a data breach. Where possible, it should first confirm that the data breach has occurred. It may make sense for the DBT to

proceed Contain the Breach on the basis of an unconfirmed reported data breach, depending on the likelihood of the severity of risk.

CONTAIN THE BREACH

The DBT should consider the following measures to Contain the Breach, where applicable:
Shut down the compromised system that led to the data breach.
Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (eg: remotely disabling / wiping a lost notebook containing personal data of individuals.)
Prevent further unauthorized access to the system.
Reset passwords if accounts and / or passwords have been compromised.
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.

ASSESS RISKS AND IMPACT

Knowing the risks and impact of data breaches will help Law Firm determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

<u>Risk and Impact on Individuals</u>

How many people 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?
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? eg: a lost device protected by a strong password or encryption could reduce the impact of a data breach.

<u>Risk and Impact on organizations</u>

What caused the data breach?
Determining how the breach occurred (through theft, accident, unauthorized access, etc.) will help 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 Law Firm 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, affected individuals must be notified 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.

REPORT THE INCIDENT

Law Firm is legally required to notify affected individuals if their personal data has been breached. This will encourage individuals to take preventive measures to reduce the impact of the data breach, and also help Law Firm rebuild consumer trust.
Who to Notify:
Notify individuals whose personal data have been compromised.
Notify other third parties such as banks, credit card companies or the police, where relevant.
Notify GDPR especially if a data breach involves sensitive personal data.

The relevant authorities (eg: police) should be notified if criminal activity is suspected and evidence for investigation should be preserved (eg: hacking, theft or unauthorized system access by an employee.)

When to Notify:
Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
Notify affected individuals when the data breach is resolved

How to Notify:
Use the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify:
How and when the data breach occurred, and the types of personal data involved in the data breach.
What Law Firm has done or will be doing in response to the risks brought about by the data breach.
Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
Contact details and how affected individuals can reach the organization for further information or assistance (e.g. helpline numbers, e-mail addresses or website).

EVALUATE THE RESPONSE & RECOVERY TO PREVENT FUTURE BREACHES
After steps have been taken to resolve the data breach, Law Firm should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which led to the data breach.

Operational and Policy Related Issues:
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, networking, or connectivity to the Internet?
Were the methods for accessing and transmitting personal data sufficiently secure, eg: access limited to authorized 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 sufficient resources allocated 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?

Monitoring

Everyone must observe this policy.

The DPO has overall responsibility for this policy.

The DPO will review and monitor this policy regularly to make sure it is effective, relevant, and adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organization at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

Data Breach Notification Form