KGB Cleaning South West Ltd
General Data Protection Regulations 2018
Data Protection Breach Policy

Introduction
The General Data Protection Regulations 2018 requires that KGB Cleaning South West Ltd provides assurance that appropriate procedures are in place for the handling of security incidents involving Personal Data. It's purpose is to enable organisations to measure their compliance against the legislation and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

This policy is effective from the 25th May 2018 and will be reviewed on an annual basis.

The purpose of an incident response is to ensure that:
- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure.
- Mitigation improvements are made and put in place to prevent recurrence.
- Serious breaches can be reported to the Information Commissioner's Office (ICO).
- Learnings are communicated to the organisation as appropriate to prevent future incidents.

Intended Audience
The intended audience for this document is anyone involved in responding to a data protection breach.

Scope
This procedure applies to all staff, partners, shared services, suppliers, contractors, representatives and agents of KGB Cleaning South West Ltd who process personal data for which KGB Cleaning South West Ltd is either the data controller or has an interest in the personal data affected. All staff have a role to play to ensure a safe and secure workplace

Terminology
In line with International Organisation for Standardisation (ISO) directive on the use of terminology in standards and for the avoidance of doubt the following words have the specific meanings ascribed below when used in this document:
- 'Shall' or 'Must' denote a mandatory requirement. Deviation from these shall constitute non-conformance.
- 'Shall Not' or 'Must Not' denotes something that is prohibited.
- 'Should' denotes a recommendation that is non-mandatory.
- 'Should Not' denotes something that is not recommended.
- 'May' denotes something that is optional.

Incident Management - Definition
A Data Protection breach is the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or inappropriate processing that

results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the Personally Identifiable Information (PII).

Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent reoccurrence of the event.

Examples of common incidents are listed below:

Type	Example
Technical	Data Corruption
	Malware
	Corrupt Code
	Hacking
Physical	Unescorted visitors in secure areas
	Break-ins to sites
	Thefts from secure sites
	Thefts from unsecured vehicles/premises
	Loss in transit/post
Human	Data Input errors
	Non-secure disposal of hardware or paperwork
	Unauthorised disclosures
	Inappropriate sharing
	Unsecured devices or documentation

ALL suspected data protection breaches must be reported either verbally or in writing to their Line Manager or Data Protection Officer.

Management Statement of Intent - KGB Cleaning South West Ltd shall:

- Put measures in place to ensure that awareness of data protection will enable breaches to be reported more easily.
- Issue guidance on how to report Personally Identifiable Information (PII) breaches for analysis, categorisation and response.
- Provide resource to analyse reported Personally Identifiable Information (PII) breaches to identify those that are incidents requiring a structured response.
- Assemble breach response teams with a defined responsibility assignment matrix, as required, to contain and recover from security incidents.
- Ensure that contemporaneous logs of incidents are kept.
- Hold periodic post resolution lessons learned meetings to focus on trends and improvements to reduce the likelihood and impact of reoccurrence, as appropriate.

KGB Cleaning South West Ltd recognises that in some instances Personally Identifiable Information (PII) breaches are beyond its reasonable control and the importance of being prepared for such eventualities.

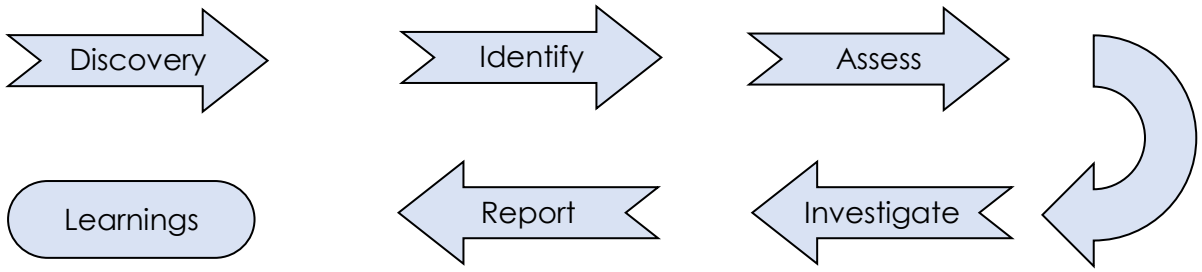
KGB Cleaning South West Ltd
General Data Protection Regulations 2018
Data Protection Breach Policy

KGB Cleaning South West Ltd shall ensure that it reacts appropriately to any actual or suspected Personally Identifiable Information (PII) breaches occurring either within KGB Cleaning South West Ltd, its systems or with data processors.

KGB Cleaning South West Ltd recognises that a structured response to Personally Identifiable Information (PII) breaches has a number of clear benefits to it including:

- Improving overall Personally Identifiable Information (PII) security.
- Reducing adverse business impacts.
- Strengthening the Personally Identifiable Information (PII) breach prevention focus.
- Strengthening prioritisation.
- Strengthening evidence collection and custody arrangements.
- Contributing to budget and resource justifications.
- Improving updates to information governance risk assessment and risk management.
- Providing Personally Identifiable Information (PII) security awareness and training material.
- Providing input to Personally Identifiable Information (PII) security policy reviews via lessons learned.

Flow Process for Personally Identifiable Information (PII) breach incident:



Discovery
Breaches and weaknesses need to be reported at the earliest possible stage to your Line Manager or the Company's appointed Data Protection Officer, either verbally or in writing, following notification, the Data Protection Officer will open an incident log

Identify
The Data Protection Officer will identify the details of the breach:

- Type of breach.
- Person/s involved.

Assess
The Data Protection Officer will make an initial assessment of the breaches severity to evaluate the potential risk to the Company and will need to capture most of the information needed to establish the scope of a breach but there will be a need to obtain additional information about the event, the assets affected, determining the type of incident, its category and priority before putting together an incident response team to manage the incident.

Investigate

- Create an entry in the KGB Cleaning South West Ltd Personal Data Incident Log using the information provided by the person who reported the breach.
- Create a folder on the Company server under Data Breaches using the following format – Breach Reference Number and its breach date.
- Start an investigation report and save it in this folder together with any emails/documents relating to the breach.
- The investigation should be achieved by interviewing the key personnel involved in the breach and their Line Managers and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified.
- Inform the Data Controller and prepare report for Breach Review Meeting, if required.
- Consideration must be given to notifying the Information Commissioner's Office (ICO) and the individual(s) affected by the breach. Factors to consider include:
    - Sensitivity of Information
    - Volume of information
    - Likelihood of unauthorised use
    - Impact on individual(s)
    - Feasibility of contacting individuals
- Ensure that any learnings to prevent reoccurrence are cascaded as appropriate and with legislation.

Report

The objective of any breach investigation is to identify what actions the organisation needs to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to the Information Commissioner's Office (ICO). The purpose of the report is to document the circumstances of the breach, what actions have been taken, what recommendations have been made and whether the disciplinary action process needs to be followed.

Learnings

Key to preventing further incidents is ensuring the Company learns from an incident. Review meetings will take place chaired by the Data Protection Officer to agree recommendations and each Breach Report will be shared with the Board and its Directors. These meetings will consider trends and identify opportunities for improvement.

Not all data protection breaches will result in formal action. Some will be false alarms or 'near misses' events that do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these will allow lessons to be learnt and continual improvement.

A culture in which data protection breaches are reported should be fostered. Although sanctions cannot be totally ruled out, the key objective is to develop a valuable insight into how such events occur and staff need to be assured that reporting a breach will not be in itself result in disciplinary action.

Incident Review

A key part of data protection breach management is a process of continual review. Every two to four weeks the Data Protection Officer and Directors meet to review current breaches. The purpose of these meetings is to provide an update on the progress of any investigation, discuss possible recommendations and consider whether specific incidents should be reported to the Information Commissioner's Office ICO.
These meetings are used to review the outcome of any investigations, as appropriate, and examine the recommendations made and discuss information governance matters. Following on from these meetings, a monthly brief is given of an overview of current issues and breaches which are then escalated to the Board and its Directors, if required.

Recommendations

Regardless of the type and severity of incident, there will always be recommendations to be made even if it is only to reinforce the existing procedure. There are two categories of recommendation that can be made:

- Local – these apply purely to the department(s) affected by the incident and will usually reflect measures that need to be taken to restrict the changes of the same type of incident occurring.
- Corporate – some incidents will be caused by factors that are not unique to one department but can be found right across the Company. Issues such as training, information handling and physical security affect all departments and it is essential that the Company identifies such risks and puts in place measures to prevent the incident occurring elsewhere. Corporate recommendations may be shared regionally especially where it relates to policies/protocols in use by a number of public bodies.

All recommendations will be assigned an owner and have a timescale by when they should be implemented. This will have a dual purpose, the first is to ensure that the organisation puts in place whatever measures have been identified and that there is an individual that can report back to KGB Cleaning South West Ltd on progress. The second is that where incidents are reported to the Information Commissioner's Office (ICO) KGB Cleaning South West Ltd can demonstrate that the measures have either been put in place or that there is a documented action plan to do so.
This is a recurrent theme of ICO enforcement and it is important that the Company's procedures reflect this. Identifying recommendations is more than just damage control, its the knowledge of what has happened together with the impact is a fundamental part of learning which can then be disseminated throughout the Company.

John Nicholls, Managing Director

25th May 2018