JOE & THE JUICE

PERSONAL DATA BREACH RESPONSE PROCESS

Title: Personal Data Breach Response Process
Effective Date: October 2025
Review Date: October 2026
Process Owner: Compliance
Approved by: Selby Marshall

Contents

1 About this document

1.1 Document history

Date	Version	Release Notes	Author
October 2025	1.0.0		• Bree Bakaric

1.2 Contributors

Name	Role
• **Bree Bakaric**	• Senior Data Privacy & Compliance Associate

1.3 Reviewers

Name	Role
• **Bree Bakaric**	• Senior Data Privacy & Compliance Associate
• **Selby Marshall**	• Head of Risk, Compliance & Safety

2 Introduction

2.1 Purpose & Scope

The purpose of this policy is to outline the internal process JOE & THE JUICE will follow in the incidence of an internal or external data breach. This process has been designed to ensure that when we become aware of a possible or actual data breach, the business can rapidly act to mitigate associated risks & protect stakeholders. The process aims to rapidly detect, assess, contain & respond to data breaches in order to minimise damage, preserve data, ensure regulatory compliance, maintain trust in the brand & enable continuous improvement in respect to our handling of data.

2.2 Roles and responsibilities

It is the responsibility of all employees to be alert & aware of the potential of data breaches & to notify the incident response team when a suspected, or actual, data breach has occurred (via the Incident Response form linked at Appendix A).

The incident response team shall be comprised of the Compliance team & relevant IT personnel.

The data response breach process will be a joint venture between Compliance & IT, with Compliance managing the regulatory & stakeholder communications & IT managing containment of the breach, recovery efforts & implementation of further security measures. Both Compliance & IT will engage in collaborative post-incident review to minimise the risks of future incidents.

Responsible	Responsibilities
• **Joe & The Juice Compliance Team**	• Yearly review & Personal Data Breach Response Process Approval • Empower employees to report data breaches • Inform, train & guide on Personal Data Breach Response Process
• **Joe & the Juice IT Team**	• Assist with Personal Data Breach Response Process • Contain data breaches
• **Joe & The Juice Employees**	• Know, Understand & Comply with Personal Data Breach Response Process

2.3 Reviews

This document shall enter into force, unless otherwise indicated, on the day of its approval and shall remain valid until it is modified or revoked in a subsequent document.

This document may be repealed in whole or in part by the competent area that approved it and in a subsequent document that expressly so states in a repealing provision.

This document will be reviewed at least once a year.

3 Detecting a Personal Data Breach

Data breaches can occur in a variety of ways & range from small incidents, such as the accidental sending of an email containing personal information to an incorrect recipient, to larger scale incidents, such as unauthorised access & theft of widespread customer credit card details via malicious software.

Data breaches are not only unauthorised access or sharing of data but also include the accidental or unlawful destruction, loss, alteration or disclosure of personal data.

Examples of potential data breaches to be aware of include the following:

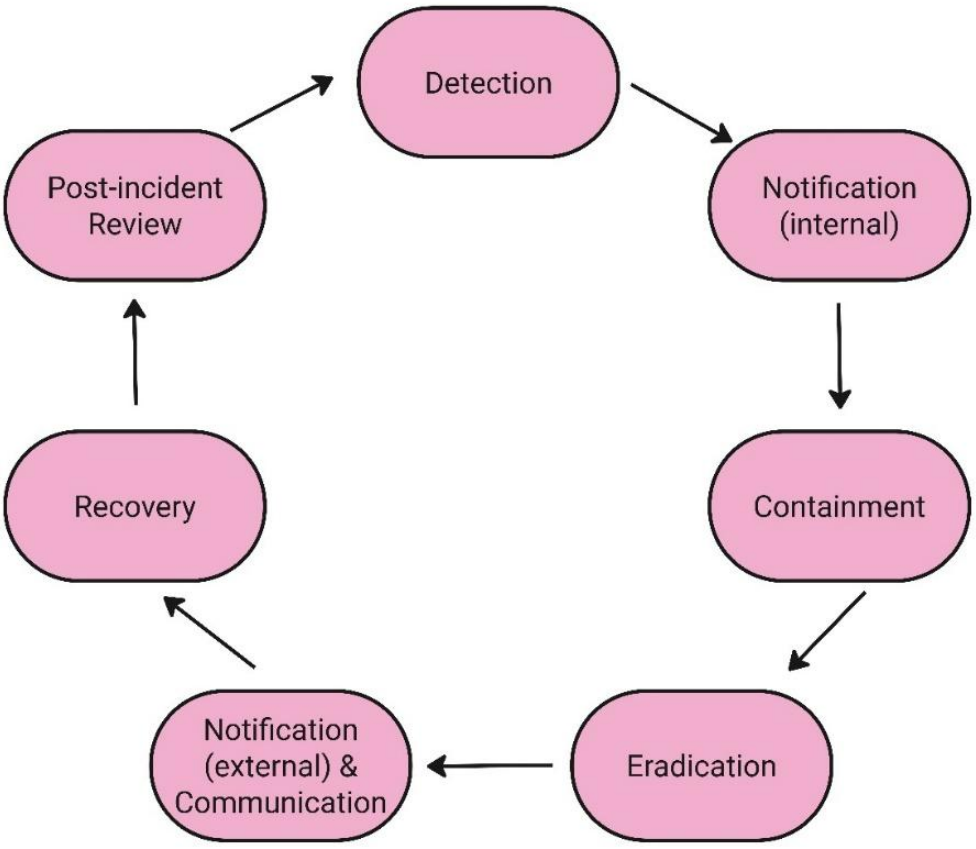
- Potential cyberattacks such as malware/ransomware, phishing, credential theft,
- Accidental deletion of data
- Sending personal data to an incorrect recipient
- Loss, theft or destruction of physical device (e.g. – laptop, phone, hard drive/USB or physical document containing personal data)
- Unauthorised access to software system containing data
- Stolen passwords or leaked credentials
- Malicious software installed on computer
- Accidental alteration of personal data stored
- Alteration of personal data without permission

- Improper or inappropriate usage of personal data collected (e.g. – using personal data of others for uses other than the purpose for which it was collected)

4 Incident Response Process

In order to identify & respond to data breaches as efficiently as possible & to minimise the scope of any potential loss of data, we employ the Detect, Respond, Recover, Learn & Improve model, detailed below.

The aim of this model is to identify potential data breaches as soon as possible & to notify IT & Compliance immediately (even in situations where it is uncertain if a breach has occurred) – It is better to be safe than sorry! A risk assessment of the potential impact & severity of the breach must be performed when a data breach is identified. The likelihood & severity of the risk to the rights & freedoms of the data subject[1] should be determined by reference to the nature, scope, context & purposes of the data processing.



[1] The rights & freedoms of data subjects in relation to their personal data include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restriction of data processing, the right to data portability & the right to object.

Steps	Detailed Process	Responsible Parties
1 Detection & Notification (internal)	• Identify & confirm incident has occurred • Complete Incident Response form at Appendix A & send to Compliance team immediately	Compliance Department where data breach may have occurred
	Compliance & IT to: • Perform Risk Assessment detailing type of breach, impact (see Appendix B) & severity of incident (Appendix C) • Assess scope of data subjects affected (including amount & geographical location) • Assess risk to rights of data subjects – based on seriousness of potential adverse consequences & likelihood of those outcomes occurring	Compliance IT
2&3 Containment & Eradication	• IT to stop ongoing malicious activity • IT to minimise loss & eliminate threat	IT
4 Notification (external) & Communication	• Notify relevant regulatory authorities if the requisite level of severity is met (see Appendices C & D) • Notify affected data subjects if threshold reached (see Appendix C) • Engaged with Brand & Comms team if press release required	Compliance Brand & Comms (if public communication required, or potential for reputation to be impacted negatively)
5 Recovery	• IT to activate data loss & recovery procedures • Restore to business activities as usual	IT
6 Post-Incident Review	• Record breach on internal register (including reasons for/against notification, impacts & action taken) • Conduct root cause analysis of breach • Fix IT vulnerabilities for future prevention of incidents • Review overall response effectiveness, identify weaknesses & improve systems (if necessary)	IT Compliance

	• Review third party partners involved in breach • Develop or improve prevention plan • Summarise learnings • Report to Risk and Reputation Committee	

Appendix A – Data Breach Incident Response Form

Please complete our Data Breach Incident Response form here - Data Breach Incident Response Form

Appendix B – Classification of Personal Data Breach Impact

Performing a risk assessment of a data breach involves assessing the potential impact & severity of the risk posed to the persons whose data has been breached. This involves consideration of the following factors:

- Type of data breach: for example, whether the breach involves company data, personal data or sensitive data.
- Nature, sensitivity & amount of personal data: the more sensitive the information contained in the data breach is, the greater the risk to the data subject. Additionally, the larger the amount of information breached & the greater the number of data subjects involved, the greater the potential impacts.
- Ease of identification: it is necessary to consider whether the data subjects can be personally identified by the data breached (either directly or indirectly).
- Attributes of data subject: if the data subjects are children or vulnerable people, the consequences may be more severe.
- Severity of consequences of data breach: generally, a persona

Examples of Incidents	**Potential Impacts**		
	LOW	**MEDIUM**	**HIGH**
Unauthorised alteration or destruction of personal data	Accidental & isolated alteration or deletion of personal data that can easily be retrieved	Ongoing, malicious or negligent alteration or deletion of personal data that involves multiple data subjects	Large scale alteration or deletion of personal data that can impact business operations
Unauthorised disclosure of data to third party	Limited to single or several data subjects/isolated event that is easily fixed	Involves a group of data subjects but has no external exposure for company	Large amount of users/data subjects impacted with potential for reputational damage
Cyber attack (hacking, ransomware, phishing, denial of service)	Limited to single or several data subjects or system users	Involves a group of data subjects or users but has no external exposure for company	Large amount of users/data subjects impacted
Any breach involving personal financial information which has potential for identity theft or fraud			
Any breach of personal data which may cause humiliation or loss of reputation to the data subject			
Any breach involving sensitive personal			

information (such as health/genetic data, ethnicity, financial data, religious beliefs, sexual orientation, political opinions)			

Appendix C – Severity of Personal Data Breach

The table below is to be used only as a general guide to when notification to data subjects and/or regulatory authorities may be required.

Whether notification is required will be determined on a case-by-case basis by the Compliance team, taking into consideration the unique circumstances of the incident and its context.

Severity Level	General Data Breach Characteristics	Is Notification to Data Subjects And/or Regulatory Authorities required?
1	Affects data or services which includes confidential company data but no personal data involved	No
2	Impacts single or few data subjects or system users but is an isolated incident & easily remediable	No
3	Alteration or deletion of large amounts of personal data accidentally	Yes, if data cannot be retrieved
4	Impacts single or few data subjects or system users but involves significant amounts of personal or sensitive data of employees, customers or third parties	Yes
	Alteration or deletion of large amounts of personal data maliciously	Yes, if data cannot be retrieved
5	Access to internal systems & large-scale personal or sensitive data by malicious third parties	Yes

Appendix D – Regulatory Notification Requirements

Country	Notification Requirements	Regulatory Body
Denmark	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Datatilsynet (Data Danish Protection Agency)
	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Norway	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Norwegian Data Protection Authority
	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Sweden	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Integritetsskyddsmyndigheten (Swedish Authority for Privacy Protection) (IMY)
	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Finland	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Data Protection Ombudsmen

	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
France	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Commission nationale de l'informatique et des libertés (CNIL)
	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Germany	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (Federal Commissioner for Data Protection and Freedom of Information)
	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Belgium	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Autorité de la protection des données - Gegevensbeschermingsautoriteit (Belgian Data Protection Authority) (APD-GBA)
	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Netherlands	Article 33 *GDPR* – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Autorieit Persoonsgegevens (Dutch Data Protection Authority) (AP)

	Article 34 *GDPR* – notification of personal data breach to data subject without undue delay	
Switzerland	*Federal Act on Data Protection* – notification of personal data breach to FDPIC as soon as possible if likely to lead to high risk of data subject's personality or fundamental rights	Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (Federal Data Protection and Information Commissioner) (FDPIC)
	Federal Act on Data Protection – notification of personal data breach to data subject if required for their protection (timely manner)	
United Kingdom	Article 33 *UK GDPR* & section 67 *Data Protection Act* 2018 – notification of personal data breach to supervisory authority without undue delay (where feasible – 72 hours) unless it is unlikely to result in risk to rights & freedoms of natural persons	Information Commissioner's Office (ICO)
	Article 34 *UK GDPR* & section 68 *Data Protection Act* 2018 – notification of personal data breach to data subject without undue delay	
United States of America	Florida – *Florida Information Protection Act* • must notify FL resident if may result in identity theft or financial harm (as soon as possible without undue delay, no later than 30 days after breach identified) • must notify Florida Department of Legal Affairs (Attorney General's office) if > 500 Floridians affected	Florida Department of Legal Affairs (Attorney General's Office)
	New York City – *New York State Information Security Breach and Notification Act* • must notify NY resident if inadvertent disclosure by persons authorised to access data & determined that data will not be misused or result in financial or emotional harm to data subjects	New York Attorney General – if breach involves personal data of NY residents Department of State – if breach involves personal data of NY residents

	• must notify NY Attorney General's office, Department of State, NY State Police if any NY residents to be notified (without unreasonable delay), must notify NY Attorney General's office if >500 NY residents affected but determination not to disclose to data subjects made (within 10 days after determination)	New York State Police – if breach involves personal data of NY residents
	Washington – *Washington State Data Breach Notification Act* • must notify WA resident if personal data was acquired by unauthorised person & data was not secured (e.g. – encrypted) but not required if breach not reasonably likely to subject consumers to risk of harm • must notify Attorney General's office if >500 WA residents must be notified of breach (as soon as possible without unreasonable delay, no more than 30 days after breach discovered	Washington Attorney General
	California – *California Data Breach Notification Law* • must notify data subject if CA resident whose unencrypted personal information was acquired by unauthorised person • must notify Attorney General if required to notify >500 CA residents (as expediently as possible without unreasonable delay)	California Attorney General
	Minnesota –*Minnesota Stat. § 325E.61* • must notify MN resident if their unencrypted personal information was acquired by unauthorised person • must notify nationwide consumer reporting agencies if >500 persons must be notified (within 48 hours)	
	Illinois – *Illinois Personal Information Protection Act*	Illinois Attorney General

	• must notify IL resident of breach following discovery when there is unauthorised acquisition of personal information that compromises the security, confidentiality or integrity of the data • must notify Attorney General if required to notify >500 IL residents (in the most expedient time possible without unreasonable delay, but no later than when consumers notified)	
	Pennsylvania – *Pennsylvania Breach of Personal Information Notification Act* • must notify PA resident & consumer reporting agencies of breach of unencrypted & unredacted personal information that has been access/acquired by unauthorised person & may cause loss or injury • must notify Attorney General if required to notify >500 PA residents	Pennsylvania Attorney General