Comhairle Cathrach na Gaillimhe
Galway City Council

Data Breach Policy and Procedure

Contents

Introduction 4
Who is covered by this policy? 4
What documents or systems are covered by this policy? 4
What documents or data is not covered by this policy? 4
Who to contact if you suspect a data breach? 4
What is a data breach? 5
Types of data breaches 5
Impact of data breach. 5
Procedure for dealing with Data Breaches 5
Data Security 5
Steps for dealing with a breach. 6
Conditions where Notification is not required 7
Yearly Review 8
Records Retention 8
Appendix 1 9
Appendix 2 10

Acronyms

Galway City Council	GCC
General Data Protection Regulations	GDPR
Data Protection Commission	DPC
Data Protection Officer	DPO
SAR	Subject access request
Subject Access Requests	SARs
Data subject access request	DSAR
Information Technology	ICT
Charter of Fundamental Rights	The Charter

1. Introduction

This policy is to provide staff, customers and third parties with guidance on our procedures for preventing and dealing with possible breaches of personal data held by Galway City Council.

Galway City Council (GCC) are a local authority that collect personal data and special categories of personal data on our customers. This data is used to provide our customers with the provision of essential services within our area of responsibility.

Any data breach that may occur could have an impact on the privacy rights of our customers. Such a breach could impact their right to private and family life, home and communication (Article 7 Charter of Fundamental Rights).

GCC endeavours to ensure that all personal data and special category of personal data on our customers is safe and secure and that we comply with our obligations under General Data Protection Regulations (GDPR). However, GCC acknowledges that breaches can occur, and that our customers may be impacted adversely when a breach of personal and/or special category of personal data is made by GCC.

We may also have access to personal data of third parties and we endeavour to ensure that this data is kept safely and securely and any breaches that may occur can impact on their Article 7 rights and this policy applies to third party data held by GCC.

2. Who is covered by this policy?

This policy covers all staff working in GCC, our customers, any third parties whom we transfer data to or any third-party processors and third-party service providers who access GCC buildings.

3. What documents or systems are covered by this policy?

All personal data and special categories of personal data that is held by GCC is covered by this policy.

This policy also covers staff who work remotely. Where equipment is provided by GCC's ICT team to **staff**, this policy will apply to any equipment provided.

4. What documents or data is not covered by this policy?

Any data that staff upload onto their work laptops and devices such as family photos or staff using their GCC devices for non-work-related use, this policy will not apply to such data. Where a loss or breach of non-worked related data, this loss or breach will not be considered a breach of data under this policy and this policy will not apply to this type of data.

5. Who to contact if you suspect a data breach?

If you suspect or believe that a data breach has occurred, you should immediately contact your line manager and your line manager should e-mail the dpo@galwaycity.ie about your suspicions. The Data Protection Officer (DPO) will liaise with you and your line manager regarding the breach.

6. What is a data breach?

Article 4(12) of GDPR states that a personal data breach is:

“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, transmitted, stored or otherwise processed”.

7. Types of data breaches

There are 3 types of personal data breaches:

1. Confidentiality breach- where there is an unauthorised access or disclosure of, or access, to personal data.
2. Integrity breach- where there is an unauthorised or accidental alteration of personal data.
3. Availability breach- where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

GCC are susceptible to all 3 types of breaches, but confidentiality and availability breaches are the most likely to occur.

8. Impact of data breach.

Recital 85 of GDPR states that a personal data breach that is not dealt with in timely fashion can result “in physical, material and non-material damage to a natural person”. The risk of a breach on customer, staff member or third-party could result in the limitation to their privacy rights, cause identity theft, induce fraud and financial loss. There is a potential that a breach could result in economic and/or social disadvantage to customers, staff members and third-parties.

As GCC has a large number of customers from disadvantaged backgrounds and from ethnic minority backgrounds, a breach of personal data could seriously impact these services users adversely.

GCC also retains data on all staff working within the organisation. The data on the files can contain special categories of personal data and the impact of the loss or unauthorised access to or alteration of this data could be seriously detrimental to staff within the organisation.

9. Procedure for dealing with Data Breaches

Under Article 33 of GDPR, a data breach must be reported to the Data Protection Commission (DPC) within 72-hours after becoming aware of the data breach. Recital 82 states that GCC should “ascertain whether all appropriate technological and organisational measures have been implemented to ascertain” that a personal data breach has occurred.

Even when a staff member is unsure of whether a breach has occurred, the staff member should contact the DPO and provide all information pertaining to the possible breach. The DPO has 72-hours to report breaches to the DPC. The 72-hours includes **weekends and bank holidays.**

10. Data Security

All staff will ensure that data sent internally and externally is given to the person(s) entitled to receive it. A staff member should not send customers’ personal data to “AllStaff” within the organisation or to “AllStaff” within their section. Data should only be provided to the relevant staff that need to access to the data as part of their duties.

If staff are sharing special categories of personal data or personal data of a customer externally, this data should be encrypted/password protected or sent by registered post. When a data subject is seeking their personal data, the documents should be password protected when sent by e-mail or the documents should be sent by registered post.

When sending out general information to the public of campaigns being carried out by Galway City Council via mailing lists, staff should e-mail these by using the **BCC function.**

As GCC is moving to a cloud-based system, attachments should not be sent by e-mail internally. A link should be copied to the body of the e-mail. Staff should utilise this link function rather than attach documents to e-mails.

All line managers should ensure that only authorised staff are entitled to access to the folders on Sharepoint that are required for their roles. If staff transfer or change roles within their section, transfer to a new section or are promoted within GCC, managers should ensure that a review is carried out on the access to Sharepoint folders. Access should be removed from staff who are no longer entitled to access to Sharepoint folders if it is not part of their new role then access should be removed where a staff member has moved to a new role within the section or promoted to a different section within GCC.

11. Steps for dealing with a breach.

Step 1

Once a staff member becomes aware of a breach, the staff member should inform their line manager. The DPO should also be informed immediately about the breach. These steps apply to data breaches relating to staff members of GCC.

Step 2

Both the line manager and the staff member who first becomes aware of the breach should carry out an investigation to determine the nature of the breach, the type of data that has been disclosed and the potential impact that the unauthorised release of the personal data could have on the person affected by the unauthorised release.

Step 3.

If the breach relates to an e-mail, the staff member should recall the e-mail and delete it from the account that it has been sent to. If they are unable to carry out a recall, they should contact the person whom they sent the data to, request that they delete the e-mail from their system. When contacting a person to delete the e-mail, a staff member should either obtain written confirmation that the e-mail was deleted or send an e-mail confirming the contents of the phone call so as to have a record of the conversation.

Step 4

The line manager and the staff member should complete the breach incident form as set out in appendix 1 and submit to the DPO without delay on becoming aware of the breach. This will be used by the DPO to review the incident and to determine whether any further steps are required to be taken.

Step 5

Where customers personal data or special categories of personal data has been breached, the staff member and/or line manager must immediately inform the DPO of the breach. The DPO must then inform the person affected by the breach. Communication to the affected party should always be in writing. The letter should include details of the breach, an apology and contact details for the Galway City Council DPO and the Data Protection Commission. A template letter is set out at appendix 2 below.

Where an affected party cannot be identified or is unknown to GCC staff, there is no requirement to inform the affect party of the data breach. However, the DPC must be informed of the data breach where it has an impact of the rights of the affected party.

Step 6

After receiving the report (appendix 1), the DPO will assess the impact of the breach, the mitigating factors, the steps to be taken and any other relevant factors pertaining and determine the risk rating of the breach.

Step 7

If the breach is medium to high the DPO must inform the Data Protection Commission within 72-hours. Minor or low risk breaches will not need to be reported to the DPC.

Step 9

All breach notifications will be retained by the DPO on a register.

12. Conditions where Notification is not required to DPC

All breaches medium to high risk breaches should be notified to the DPO. However, a notification to the DPC of a data breach is not required to be made where the following conditions are met, as per article 34(3) of GDPR:

(a) The controller has implemented technical and organisational protection measures and these 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
(b) The controller has taken subsequent measures which ensure that the high risk to the rights freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise
(c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

GCC will ensure that all personal and special categories of personal data is protected from unauthorised access by third parties and that all security and/or protective measures are put in place to protect this data.

Where a notification may involve a disproportionate effort in contacting customers or members of the public, GCC will publish details of any breaches so that customers/members of the public are aware of the data breach and are informed as to whether their rights and freedoms have been affected by the breach.

13. Yearly Review

An annual review will be conducted by the DPO to determine the nature and type of breaches that regularly occur within GCC. After completion of this yearly review, the DPO will organises specific training and information sessions with all GCC staff regarding breaches and how to mitigate same.

14. General

The DPO will carry out regular audits, training and information sessions for staff in regard to breaches and advise staff regularly on the appropriate steps to be taken in relation to breaches and on the best practices for protecting the data on GCC systems.

15. Records Retention

Records in relation to a breach incident will be kept for a period as set out in the retention schedules and if a litigation exceeds the retention schedule, the data will be kept until all appeal avenues have been exhausted.

16. Related Documents

Data Protection Policy

Data Subject Rights Policy

Privacy Notice

Appendix 1

Data Breach Incident Report Form

Details of staff & section notifying breach			
Section		Date	
Staff member		Line Manager	
Details of Incident			
Date you first became aware of breach:			
Details of Breach:			
What types of data was breached	Personal Data	Sensitive Personal Data	Non-personal
Mitigation steps	Recall/deletion of e-mail	Request to destroy/request to return data	Data was encrypted
Was the Data Subject informed	Yes	No	Unable to contact Data subject as unknown:
What date was Data subject informed		Was it in writing or by phone call?	
Steps taken to mitigate future breaches, please provide details			
Signed			
Line Manager		Staff Member	
Dated		Dated	
DPO Review			
Impact of breach	Rating of breach	Inform Data subject	Inform DPC
Reason for decision			
Mitigation	Type of data	Impact of breach	Other factors
Signature and date by DPO			
Signed			
Dated			

Appendix 2

Template Letter

Date:

Our reference:

Dear Sir/Madam,

I am writing to inform that on the…day of….., 202…. Galway City Council discovered a data breach relating to your personal data. The following data was released to a third party:

1. Description of the breached data that was released. Give a list of the type of data released.

2.

Due to an error by Galway City Council in inputting the address/e-mail address or inadvertently including the documents with your personal data on a letter/e-mail addressed to another customer, your data was sent to an unintended recipient (please amend this to reflect how the breach occurred, ensure that you don't identify the staff member but refer to Galway City Council staff)

Galway City Council has retrieved and/or requested the destruction/deletion of the data that was sent to the unauthorised recipient. Galway City Council has received confirmation from the authorised recipient that they have deleted/destroyed/returned the data.

Galway City Council has implemented procedures to ensure that a similar does not occur again.

We wish to unreservedly apologise for the breach. You can contact Galway City Council Data Protection Officer via e-mail dpo@galwaycity.ie, by phone on (091) 536400 or by post marking the letter for the attention of the Data Protection Officer.

You can also make a complaint to the Data Protection Commission at the below address:

Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28

info@dataprotection.ie

www.dataprotection.ie - Data Protection Commission

+353 (0)761 104 800

+353 (0)57 868 4800

Yours sincerely,

_____