50808 Data Policies

This policy is relevant to the spunout (Community Creations CLG) service 50808. Community Creations is undergoing a rebrand which will result in a name change to spunout. Once the legal name change has taken place this policy will be updated. 50808 and spunout.ie are currently trading names of Community Creations CLG.

Table of Contents

Section 1: Data Policy

This policy is relevant to the spunout (Community Creations CLG) service 50808. Community Creations is undergoing a rebrand which will result in a name change to spunout. Once the legal name change has taken place this policy will be updated. 50808 and spunout.ie are currently trading names of Community Creations CLG.

1.1. Introduction

Under the Data Protection Acts 1988 and 2003 and the General Data Protection Regulation (GDPR), 50808 has certain obligations placed on it as a Data Controller to process personal data in a fair and transparent manner.

50808 is committed to best practice in data protection and all data retained by the organisation will be kept no longer than necessary to achieve the stated purpose for which it was originally collected.

The term “data subject” refers to any living human whose personal data might be collected or processed by 50808. The “Data Protection Officer” will be an assigned member of 50808 staff with responsibility for certain processes outlined in this document.

1.2. Data Collection

“Personal data” refers to any information which can be used to identify a living person. Personal data can only be collected and processed by 50808 if doing so satisfies one of the following conditions:

A. Consent has been received from the data subject that their personal data can be stored and processed for a stated purpose
B. The data is required for the performance of a contract
C. 50808 has a legal obligation to do so
D. 50808 has a vital interest in doing so
E. There is a public or legitimate interest in doing so

Some forms of data are categorised as “sensitive personal data”, which have stricter rules for collection and processing. Sensitive personal data is any information which records a living person’s:

- Racial or ethnic origin
- Political, religious or philosophical beliefs
- Trade union membership
- Physical or mental health condition
- Sexual life information
- Criminal record or accusations of a criminal offence
- Genetic or biometric data

50808 can only collect and process sensitive personal data if doing so satisfies one of the following conditions:

A. Explicit (clear, unambiguous) consent has been received from the data subject that their personal data can be stored and processed for a stated purpose
B. It is necessary for 50808 to fulfil its obligations as an employer or under social security/social protection law
C. It is necessary to protect the vital interests of the data subject or of another person, and the data subject is incapable of giving consent
D. The data is being used for legitimate activities arising from our status as a not-for-profit body, the data subjects are individuals with a regular connection to 50808, and the personal data is not being shared outside of the organisation
E. The data has clearly and obviously been made public by the data subject
F. It is necessary for the purpose of a legal claim
G. It is necessary for reasons of substantial public interest (while respecting and safeguarding as far as possible the rights of the data subject)
H. It is necessary for certain medical reasons, including the assessment of the working capacity of an employee
I. It is necessary for public health reasons
J. It is necessary for archiving purposes in the interest of the public, scientific or historical research, or certain statistical purposes (while respecting and safeguarding as far as possible the rights of the data subject)

In all cases of personal or sensitive data collection, the preferred condition for collection and processing by 50808 is that consent has been received by the data subject.

1.3. Data Processing

"Data processing" refers to any operation performed on personal data, e.g. collection, recording, organising, structuring, storage, adaptation or alteration.

50808 can only process personal data for the specific purpose or purposes for which it was originally gathered. Personal data should only be retained by 50808 for as long as it takes to fulfil this purpose and no longer, or until the data subject makes a legitimate request to exercise their right of erasure.

1.4. Data Storage

All personal data held by 50808 must be stored in a secure manner. Data should only be accessible to appropriate named members of staff for whom accessing the data in question forms a part of their job.

Be advised that 50808 is required to retain certain records containing personal information for a pre-set amount of time to satisfy our legal obligations. Premature destruction of such data could result in serious repercussions for the organisation. Members of staff who are in any way unsure as to whether a document should be destroyed or retained should bring their concerns to the Executive Director without delay.

1.5. Data Access Requests

Any individual whose personal data is held by 50808 has a right to request a copy of all their personal data currently held by the organisation. The information must be clear, free, comprehensive, explain the purpose for which their data is being processed, and be delivered within one month of their initial request.

50808 staff who receive a data access request must use the following step-by-step procedure:

1. Notify the Data Protection Officer (DPO) that a data access request has been received as soon as possible, preferably immediately, by emailing dpo@spunout.ie
2. The DPO will attempt to determine whether the individual who made the request is definitely the subject of the data in question; the DPO will request clear identification which may include a passport or other form of state-issued I.D., and, if deemed necessary, proofs of address, as well as requesting clarification, if needed, on the nature of the individual's relationship or former relationship with 50808
3. If the DPO is satisfied with the above, they will identify the member of staff best placed to handle the data access request
4. The designated member of staff will acknowledge receipt of the request to the requester, and inform them of the timeframe (no more than one month from the original staff member receiving the request) in which they can expect a full reply
5. If necessary, confirm the identity of the person making the request beyond reasonable doubt
6. Agree a timeframe with DPO for collation of all information held by 50808 on the requester, treating one month as an outer limit for delivery. If possible, the process should be completed well in advance of one month.
7. The designated member of staff will raise the issue with the wider team, after which members of staff will search their records for relevant data and share any such data with the designated member of staff as soon as possible
8. Upon completion of the data file, the designated member of staff must state in writing that no additional data has been withheld to their knowledge

9. With the approval of the DPO, the file containing all relevant data will be sent to the requester.

1.6. Right of Erasure

50808 recognises the legal right of data subjects to be forgotten, withdrawing their consent for 50808 to hold and process their personal data. All individuals with personal data held by 50808 may request at any time that all data held on them by the organisation be destroyed.

Data subjects are free to exercise this right, except in cases where to destroy such data would violate 50808's legal obligations, i.e. in the case of employee contractual information, which must be held for a period of years even in the event of an employee ceasing their period of employment with the organisation.

1.7. Data Destruction

Personal data held by 50808 which has served the purpose for which it was collected must be destroyed. Likewise, personal data on which a legitimate right of erasure claim has been made must also be destroyed.

The destruction of personal data stored in paper form must be conducted by shredding. Where personal data is stored electronically, care must be taken to ensure it is properly and entirely deleted from all sources and by all employees of 50808.

In the event of legal proceedings being launched against 50808, the CEO may instruct members of staff to cease any data destruction operations currently underway. Destruction should resume as soon as legal proceedings have come to a close.

1.8. Data Retention Periods

Different categories of personal data must be retained by 50808 for different periods of time in order to fulfil their purpose. In general, records should not be retained if there is no clear business reason for doing so.

Data Type	Retention Period
Child Protection Documentation	Indefinite

“Withholding” Documentation §	Indefinite
Contractual and Audit	Up to seven years from year of issue
Insurance information	Seven years from date of issue, or longer/indefinite if required by policy
HR for roles funded by grant	Up to seven years from termination of grant
Garda Vetting	Until individual’s involvement with organisation ends
Other	Until purpose for collection expires, or consent is withdrawn

§ “Withholding Documentation” refers to written records of decisions by 50808 not release personal data as requested; i.e. in a case where a data access request is made but the organisation was not satisfied of the requesting individual’s identity.

1.9. Data Breaches

A “personal data breach” is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” by 50808. Data breaches can be large or small in scale: for instance, accidentally cc’ing instead of bcc’ing people in an email could constitute a personal data breach.

In the event any member of staff becomes aware of a possible personal data breach, however small, they must inform the Data Protection Officer without delay.

Upon being notified of a potential personal data breach, the DPO must determine the following:

A. Whether there has been a breach of personal data held by 50808 or, if this cannot be definitively proven, whether it is likely such a breach has occurred;
B. Whether this breach or likely breach is damaging to the individuals whose personal data has been compromised;
C. As far as possible; who accessed what data and when, how that data is being used, and which individuals are likely to be affected.

The DPO must assess whether the data breach is significant enough to bring to the attention of the Data Protection Commission based on A, B and C, and if so must inform the Commission within 72 hours. If, for whatever reason, the Data Protection Commission is not notified within 72 hours, the DPO must include

reasons for the delay with their submission. The DPO will also inform the affected individuals whose data has been compromised.

The DPO's notification must include the following information:

1. A description of the nature of the breach including, if possible, the categories and approximate numbers of individual data subjects and/or data records involved;
2. The name and contact details of the DPO or another person who can be contacted for more information;
3. The likely consequences arising from the breach;
4. A summary of the measures taken and proposed to be taken to address the breach and, where possible, to mitigate its possible effects.

Once all relevant parties have been informed, the DPO will work with relevant staff to implement the proposed measures to address the personal data breach, including revision of policies and practices as necessary and subject to the normal processes of 50808 policy change.

1.10. Data Sharing

In some cases, 50808 may engage in peer-to-peer relationships with other organisations in which data is shared between both parties, and both become responsible for the proper use and protection of that data. All such relationships require a Joint Controller Agreement (otherwise known as a Data Sharing Agreement) to be agreed and in place before any data can be shared.

A Joint Controller Agreement must clearly set out:

- Which party is responsible for which particular elements or phases of data processing;
- Which party is responsible for responding to requests from data subjects regarding their rights, e.g. for data access requests;
- The point of contact with whom data subjects can communicate in relation to certain aspects of processing.

In other cases, 50808 may hire a third party service provider to process personal data on the organisation's behalf, with 50808 remaining responsible for the proper use and protection of the data. In order for data to be shared in such a manner, a formal Data Processor Contract must be in place with the service provider, which must include:

- The subject matter and duration of the data processing
- The nature and purpose of the processing
- The type of personal data and categories of data subjects
- The obligations and rights of 50808

Section 2: Texter Privacy Policy/Terms of Service

This policy is relevant to the spunout (Community Creations CLG) service 50808. Community Creations is undergoing a rebrand which will result in a name change to spunout. Once the legal name change has taken place this policy will be updated. 50808 and spunout.ie are currently trading names of Community Creations CLG.

Last updated: 30 April 2020

Important notices:

- *If you're at serious risk to yourself or others, we will need to reach out to emergency services to keep you and/or others safe.*
- *If you're under 18 and you tell us you are at risk of abuse or neglect, we will need to reach out to emergency and/or TUSLA to keep you safe.*
- *If you give us information about an alleged abuser, where other children may be at risk, we will need to reach out to Ireland's child protection agency TUSLA.*

2.1. Who are we?
At 50808 ("50808", "we", or "us"), our goal is to help people in crisis. We are here to help you out of a crisis – we give people the facility to reach out to a trained and supervised Crisis Volunteer whenever they need support to move from a position of crisis to a calmer, more manageable state of mind. Our organisation is called 'Community Creations CLG trading as 50808' and we are a registered charity in Ireland number 20057923.

When you send a message to 50808 to initiate a text message conversation you will receive some automated reply messages with a link to these Terms of Service.

Before using or accessing our service please read these Terms of Service. By accessing or using the Service you agree to the Terms. These Terms govern your access and use of the Service. You may contact us by e-mail at dpo@spunout.ie with questions about these Terms. If you don't agree to these Terms, you may not use the Service. If you no longer wish to receive messages, you may opt out at any time by texting the word STOP.

50808 is funded by the Health Service Executive (HSE).

2.2. How can you contact us?
Email: hello@spunout.ie for general enquiries or dpo@spunout.ie for questions about these terms.

2.3. Changes to these terms
The Terms may be changed from time to time. The most up-to-date Terms will always

be the ones that are posted here. Changes to the Terms of Service will be effective immediately upon our posting them here on our website.

On each separate occasion that you first send a message to 50808 to initiate a text message conversation, you will receive some automated reply messages with a link to our current Terms of Service so you may review them before continuing to use our service. By using our service after receiving those automated messages, you agree to the practices outlined in the current Terms.

In order to protect your anonymity, we never initiate direct contact with you. We are therefore unable to notify you directly of any changes to the Terms. Your use of the Service after such changes have been posted shall constitute your acceptance of the revised Terms.

2.4. What do we do?
We provide a text messaging service to help people who feel they are in crisis. When contacted our team of trained volunteers are there to help 24 hours a day, 7 days a week. A crisis can include difficulty dealing with stress, overwhelming feelings, symptoms of depression, anxiety, panic, self-harm, suicidal thoughts, trauma related to violence or sexual assault, or any concerns regarding your mental health or that of your loved ones.

When you send a text message to 50808, you receive a number of automated text messages. One of these contains a link to this Terms of Service document. If you do not agree to these terms of services, you can opt out at any time by texting the word STOP. If you have any questions about these terms, please email us at dpo@spunout.ie

2.5. Who do we process data about?
Other than people who work or volunteer for 50808 we only process personal data of the people who contact our service. The personal data that we hold for people who contact us is as follows:

- Your phone number
- Technical data of your message: message ID, service provider ID
- The content of your message
- Notes the volunteer might take in the course of your conversation

2.6. When will we pass your data onto third parties?
50808 respects and seeks to preserve the confidentiality of people who use our

service. We will always think carefully before we break this confidentiality. We will break confidentiality and engage with a third party in the following circumstances:

- You ask us to
- We believe that your life or the life of someone else is in danger
- You are under 18 years of age and have been hurt, abused or neglected OR are at risk of this OR have been in the past.
- You give us information about an alleged abuser, where other children may be at risk, we will need to reach out to social services.
- You tell us you are endangering the safety of another person

2.7. What do we do with your data?
When you send us a text message, our system uses your phone number to connect to our service and process our messages. Our Volunteers do not see your phone number, they will only have the information about you that you tell them directly.

50808 supervisors (paid staff) will have access to all text messages from your number. The reason for this is to make sure our texters are safe and that conversations between you and our volunteers are overseen by experienced and qualified mental health and social work professionals. Supervisors use past conversations to make decisions on reporting risk.

In some emergency situations, we will have to make a special request to access your phone number so that we can connect you to resources to help you. In a situation where a person is thought to be abusing the service, we may store some data also, for the purposes of discouraging this behaviour. More information on what we mean by abusing the service can be found below.

The system that we use records information on delivery of individual messages, like the time the message was sent, what the message was about, and the network it is delivered on. This anonymised personal data, which does not identify any individual, is used in order to learn how we can better help people who use the service. It is also used to build research into mental health trends in Ireland.

In order to provide a 24/7 service, we engage with support staff in other countries. We use technical support staff in the U.S. and in order to provide support, in some instances, they may have to access material which includes personal data.

If you choose to continue using our service after receiving our automated messages at the beginning of a conversation, you will be consenting to 50808;

- keeping all of the text messages in line with our data retention policy,

- processing and storing your telephone number including any personal or special category data that you choose to share with us, and
- to the transfer of this information to Crisis Volunteers, staff supervisors and IT support staff in countries outside the EU/EEA, which do not have equivalent data protection laws.

2.8. Abusing the service

We reserve the right to end a person's access to 50808 where that person is thought to be abusing the service. Abusing the service can mean any of the following:

- In any way using the service to break the law;
- Threatening, harassing or otherwise inappropriately communicating with volunteers or staff of 50808;
- Pretending to be another person or entity;
- Using the service to try to exploit or harm minors by exposing them to inappropriate content, asking for personal information, or otherwise;
- Taking screenshots, copying, or otherwise sharing conversations or information about the 50808 platform, except to report behaviour you believe may be illegal or abusive;
- Sending, knowingly receiving, uploading, downloading, using or re-using any content which does not comply with these terms;
- Spamming or collecting personal information of users in order to spam, market, or sell to third parties;
- Doing anything that harms anyone's ability to use our service or which we believe exposes 50808 or users of the service to liability;
- Copying, adapting, decompiling, reverse engineering, attempting to discover the source code or make a derivative work of the service or any portion of the service;
- Otherwise attempting to interfere with the proper working of 50808.

Please note that if you do choose to take a screenshot of, copy, or otherwise share or make public any part of your conversations with 50808, we cannot control what happens to that information. 50808 has no way of getting such information or images removed or withdrawn after they are made public, and we will not attempt to do so.

We reserve the right to remove from the platform any texter who makes public any aspect of their interactions with 50808, except in cases of suspected illegal or abusive behaviour.

If you do suspect illegal or abusive behaviour on the 50808 platform, you should contact senior management at dpo@spunout.ie or An Garda Síochana without delay.

2.9. Post conversation surveys
At the end of your conversation, you may receive a link to take a survey. This is to help us learn from you and improve our service.

Some policies surrounding the survey:
1. Responses are anonymous.
2. You do not have to answer all of the questions.
3. If you leave a note for your Crisis Volunteer, we'll share it with them. Your note might also be used for marketing and training.

2.10. Where do we keep your data and for how long do we keep it?
We hold all of your data securely in Ireland and Germany, and any companies who do work for us are obliged to keep your personal data in the EU/EEA. Where legal data transfer agreements outside the EU/EEA are in place, appropriate measures will be taken by 50808 in order to ensure compliance with EU Data Protection law.

We retain and store two different types of data after our conversation with you. Your Personal and Special Category Data, that is your telephone number and the record of all the text messages that you exchange with us, will be stored for up to 7 years after you last contact us. Once this time has passed, we will permanently delete this data from our records. If you contact us again after this time, you will appear to be a new service user. We will not have any record of our previous conversations with you.

We anonymise the data that is extracted from our conversations with you. This anonymised data will be retained indefinitely. This data is independent of the text record and cannot be attributed to you. We keep this data as it helps us to improve our own services and it contributes to our data set.

2.11. Do we share your data?
We will not share your personal information with anyone without your permission unless we are legally required to do so. Examples of which are when there is a child welfare concern or a concern in relation to your own wellbeing in the course of the use of the service.

We may sometimes signpost you to another service. In this instance, we will give you information on this service. We will never share your personal data with them and it is up to you whether you contact them. We do not control the privacy policy of other services.

2.12. What are your rights and who should you contact?
Individuals have rights over their personal data under EU law. These rights are not

absolute, and some qualifications and restrictions do apply.

In summary your rights are:

- Right of access;
- Right to rectification;
- Right to be forgotten / erasure;
- Right to restrict processing;
- Right to object;
- Right to refuse automated decision making and/or profiling;
- Right to portability.

You also have the right to seek compensation through the courts in the event that your data privacy rights have been infringed. 50808 is committed to helping individuals exercise their rights.

- If you want to exercise your right to access a copy of all the information we have on you email dpo@spunout.ie with the subject title 'Data Access Request'
- If you want us to erase your personal data, please text 'ERASE' to the following number: 50808. You will receive a message asking you to confirm your request. You will receive a response to your erase request within 30 days and we will make reasonable efforts to process requests promptly. If we cannot delete all of your data right away for legal reasons, you will receive an explanation of why this is the case.
- For any other queries in relation to your rights you can email us at dpo@spunout.ie

2.13. Contact Details for the Office of the Data Protection Commission (Ireland)
Webpage: www.dataprotection.ie
Telephone: +353 57 8684800 / +353(0)761 104 800
Address: Data Protection Commissioner, 21 Fitzwilliam Square, Dublin 2, D02 RD28

Section 3: Volunteer Privacy Policy

This policy is relevant to the spunout (Community Creations CLG) service 50808. Community Creations is undergoing a rebrand which will result in a name change to spunout. Once the legal name change has taken place this policy will be updated. 50808 and spunout.ie are currently trading names of Community Creations CLG.

3.1. Who are we?

50808 is a service provided by Community Creations CLG that is a registered charity in Ireland. Registered charity number: 20057923. Registered address: Sean MacBride House, 48 Fleet St, Temple Bar, Dublin, D02 T883.

50808, Inc. ("50808" or "Licensor"), available at P.O. Box 1144, New York, NY 10159, and provides technology, materials, trademarks and guidance to Community Creations CLG which company manages and operates a text line for individuals in crisis.

Community Creations CLG is a Data Controller, and pursuant to the terms of a license agreement and standard contractual clauses agreements with 50808, 50808 serves as a Data Controller and Data Processor for aspects of the data discussed herein, as defined in the General Data Protection Regulation (GDPR).

We will process the personal information you provide for our legitimate charitable interests and to enhance the experience of our volunteers. This includes contacting you about relevant volunteering opportunities, news and events.

In brief

- We respect your personal data and store it securely.
- We will never sell your personal data.
- We will remove your data if you ask us to.
- We will use your data to maintain contact with you, in order to facilitate your volunteering work with us
- We may send you content we think is relevant or interesting to you but you can unsubscribe or change your contact preferences at anytime.
- We may use your data to contact you about information you request or to allow you to access our services.

3.2 What is the purpose of this policy?

We collect and process personal information about you during and after your relationship with us in order to manage that relationship. We are committed to being transparent about how we collect and use your data to meet our obligations under the General Data Protection Regulation (GDPR).

3.3 What personal information we collect and how it is used

Personal information means any information about an individual from which that person can be identified. The information that we collect includes details such as your name, email address, physical address, postal code. The information does not include data where the identity has been removed (anonymous data).

Please view below for a list of the purposes for which we use your personal data:

Data We Collect	What we use it for	Legal basis for processing
Names, addresses, telephone numbers, email addresses	To contact you to discuss volunteering opportunities or to keep you updated on our services or activities and events; to record your location in order to understand where our volunteers come from	Justified on the basis of legitimate interest in ensuring the proper functioning of our business operations and ensuring proper communication and emergency handling. Your consent.
Curriculum Vitae or other profiles	To assess and determine your skills, experience and interests in order to assess your suitability for volunteering opportunities or specific projects	Justified on the basis of legitimate interest in ensuring the recruitment of appropriate volunteers. Your consent.
Demographics	To capture information which will help us to identify the demographics most interested in volunteering to assist future marketing campaigns To capture demographic information to ensure a broadly diverse volunteer population and to seek to rectify any under-representation of particular demographics amongst our volunteer population to help us better understand and serve diverse members of the public who reach out to our services.	Justified on the basis of legitimate interest in ensuring the proper functioning of business operations. Your consent.
Information gathered from business and social media sources in the public domain, e.g. LinkedIn, Facebook	To build a picture of your skills, experience and interests in order to assess your suitability for volunteering projects	Justified on the basis of legitimate interest in ensuring the recruitment of appropriate volunteers. Your consent.
References and garda vetting information	To assess your suitability for volunteering with us, and for being utilised on specific projects	Necessary for the compliance with a legal obligation. Justified on the basis of legitimate interest in ensuring the recruitment of appropriate volunteers. Your consent.
Information on special requirements, health or medical conditions	To assess your suitability for volunteering with us, and for being utilised on specific projects; to carry out our legal duties (e.g. to ensure health and safety)	Justified on the basis of legitimate interest in ensuring the recruitment of appropriate volunteers. Necessary for the compliance with a legal obligation. Your consent.

		your consent.
Information related to availability and the reasons for periods of unavailability	To assess your suitability for volunteering with us, and for being utilised on specific projects	Justified on the basis of legitimate interest in ensuring the proper functioning of business operations. Your consent.
IP Addresses	As an extra cybersecurity measure, we may log the IP address of the computer used to email us a contact form as part of our registration process. This type of data does not normally identify an individual in Ireland.	Justified on the basis of legitimate interest in ensuring the proper functioning of business operations. Your consent.
Content of Volunteers' conversations arising out of or concerning the services	To monitor the quality of the service provided to texters, to support Crisis Volunteers in the execution of their role, and to analyse trends and operational considerations for the improvement of the service.	Justified on the basis of legitimate interest in ensuring the proper functioning of our business operations and ensuring proper communication and emergency handling. Your consent.

3.4. Overview of the legal basis for each such purpose.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. If you fail to provide certain information when requested, we may not be able to register you for volunteering opportunities, or we may be prevented from meeting our legal obligations (such as to ensure your health and safety).

Where we rely on our legitimate interests for a given purpose, we provide (i) the transparency we provide on the processing activity, (ii) our regular privacy reviews and (iii) the rights you have in relation to the processing activity.

We will process your personal data for the purposes and on the legal bases outlined above. To the extent that prior consent is mandatory under applicable laws, processing of your data will be subject to obtaining your prior consent.

We will not use your personal data for purposes that are incompatible with the purposes of which you have been informed, unless it is required or authorized by law, or it is in your own vital interest (e.g. in case of a medical emergency) to do so.

3.5. How we use particularly sensitive personal information

We will take extra precautions to safeguard any sensitive personal information we process on your behalf. Sensitive personal information can include information on your health, race, ethnic origin, political opinions, sex life, sexual orientation or religious beliefs.

Except for certain information that is required by law, your decision to provide any personal data to us is entirely voluntary.

We will ask you for your express consent to allow us to process sensitive personal information. We will only process this sensitive personal information to process or evaluate your application, for training, quality monitoring, evaluating the services we

provide and that allow us to understand the background and experience of our volunteers. We also ask about your experiences of mental health and related services. This is to allow us to reasonably consider whether working with people in crisis might be likely to cause you (or the members of the public that we serve) physical or emotional harm.

You should carefully consider whether you wish to consent to us collecting, processing, and storing this data.

3.6. How is your personal information collected?

We collect information through our volunteer registration process, either directly from you or the references you will be asked to provide. We may sometimes collect additional information from third parties including internet, media, and social media searches such as LinkedIn. We may collect personal information in the course of volunteering activities throughout the period of you volunteering for us.

3.7. Legal basis for processing your personal data

We will process your personal data on any or all the following grounds

- Your consent - where processing is based on your consent, you have the right to withdraw that consent
- Where it is necessary for the performance of a contract;
- Where it is necessary for compliance with a legal obligation to which we are subject;
- Where it is in our legitimate charitable interests

3.8. Automated Decision Making

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

3.9. Who has access to your data?

Your information may be shared internally, including with staff members responsible for managing and administering projects, HR, health and safety, insurances, events and marketing activities.

We share your data with carefully selected third parties, including third-party service providers, including but not limited to those providers used in connection with supporting our CRM system and IT network (including remote support) and professional advisers where necessary, who may be party to confidential discussions related to an individual. In providing the Service we are supported by contractors and Licensor who are based in the United States. In order to provide support, in some cases they may have to access material which includes our volunteer personal data. We will not transfer personal data outside the European Economic Area (“EEA”)

without your permission nor without appropriate assurances on the adequacy of data privacy protection commitments.

We require third parties to respect the security of your data and treat it in accordance with the law. We will share your information with third parties where required by law, where it is necessary to administer our relationship with you or where we have another legitimate interest. All of our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

3.10. Where we store your personal data

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us, Licensor, or for one of our third party suppliers. In order to safeguard your information we will make any such transfers in strict compliance with data protection legislation with all appropriate contractual arrangements (Privacy Shield, Binding Corporate Rules, or Model Contracts) will be in place. By submitting your personal data for such purposes, you agree to this transfer, storing or processing. Community Creations will take all reasonable steps necessary to ensure that your personal data is processed securely and in accordance with this Privacy Policy.

The transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our website; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

3.11. Data Security

Community Creations CLG takes the security of your data seriously. We have internal policies and controls in place to reasonably ensure that your data is not lost, accidentally destroyed, misused or disclosed, or subject to unauthorised access. We implement appropriate network access controls, user permissions and encryption to protect data.

When we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

3.12. Data Retention

We will only retain your personal information for as long as necessary to fulfill the purposes we collected it for, including the purposes of satisfying any legal, accounting or reporting requirements. Details of retention periods, archiving and destruction policies for different aspects of your personal information are available in our retention policy which is available from the person responsible for data protection.

3.13. Your legal rights

As a data subject, you have a number of rights, details of which can be found at https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation

If you have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent at any time. Once confirmed, we will no longer process your information for the purpose you originally agreed to, unless we have another legitimate basis for doing so in law.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Data Protection Commissioner.

3.14. Accessing your data

As a matter of course, you will not have to pay a fee to access your personal information. However, if we think that your request is unfounded or excessive, we may charge a reasonable fee or refuse to comply with the request.

We may need to confirm your identity or ensure your right to exercise your legal rights. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

3.15. Changes to this policy

We reserve the right to update this policy at any time, and we will provide you with a new privacy notice when we make substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

For queries and further Information, Community Creations CLG, registered address Sean MacBride House, 48 Fleet St, Temple Bar, Dublin, D02 T883, is the Data Controller. For any queries, please contact the Data Protection Officer at dpo@spunout.ie.

Section 4: Personal Data Breach Policy and Procedure

This policy is relevant to the spunout (Community Creations CLG) service 50808. Community Creations is undergoing a rebrand which will result in a name change to spunout. Once the legal name change has taken place this policy will be updated. 50808 and spunout.ie are currently trading names of Community Creations CLG.

4.1. Purpose and Scope of this policy

This policy has been written to assist all staff and to help them follow good practice when dealing with a data protection breach and to ensure that all responses are compliant with relevant Data Protection laws. All staff are responsible for adhering to the timescales highlighted within this policy and aiding the Data Protection Officer in the course of assessing and responding to a breach.

This policy should be read in conjunction with the 50808 Terms of Service.

4.2. What is a data breach?

In Article 4 of GDPR a personal data breach is defined as;

> ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’

Where 50808 holds personal data relating to individuals, it has obligations under data protection legislation which dictates that the data in question should be held in a way which satisfies the legal basis upon which it was collected. If data is to be shared with other parties it may be subject to a contractual arrangement or for reasons set out in legislation, where there is a disclosure or use of data outside of this then a breach may have occurred.

Depending on the information held, a data protection breach may come in various forms such as a lost company laptop, an email sent to the wrong person or a hacking attempt by an outside party. The consequence of a personal data breach may be that either one or both of the Data Protection Commission and the individual whose personal data is affected by the breach may need to be contacted in order to inform them of the breach.

The 50808 is under an obligation to inform the Data Protection Commission within 72 hours of knowledge of the breach. The data subject i.e. individual concerned, should be informed as soon as is practicable. The manner of notification is outlined below.

4.3. Definitions

“Data Protection Law” means all applicable data protection law, including from 25 May 2018 the General Data Protection Regulation (Regulation (EU) 2016/679) and any legislation which amends, extends, consolidates, re-enacts or replaces same, including any statutory instruments and regulations that may be made pursuant thereto from time to time and any laws subordinate to GDPR and or enacted prior to it; and

Any reference to “Personal Data” in this agreement is to be understood to refer to “Special Categories of Personal Data” also;

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

A full set of definitions shall be found in the 50808 data privacy policy.

4.4. Roles and Responsibilities

Staff - General

a) All staff members should be made aware of the circumstances where a data breach may occur and mitigate against such a breach occurring.

b) Staff should receive adequate instruction in relation to being able to recognise a breach

c) Staff members should be clear in the importance of reporting such breaches to the Data Protection Officer should one occur and, should do so immediately where a breach has occurred.

Data Protection Officer

a) The DPO must advise on the conducting of privacy impact assessments by members of staff in any relevant areas in relation to the possibility of personal data privacy breaches occurring.

b) The DPO must give recommendations to the board and staff in relation to the measures which may be implemented in order to mitigate against possible breaches.

c) The DPO must be a clear point of contact for staff members in the event of a breach occurring.

d) The DPO must organise the actions of the 50808 in responding to a breach including acting as a point of contact with the Data Protection Commission and the Data Subject.

e) The DPO must compile a report and present it to the board in respect of any breach that occurred and any potential recommended mitigating actions that need be taken in relation to same.

The Board

a) The Board must be receptive to DPO advice and be willing to implement plans in relation to the recommendations that the DPO may have in relation to mitigating data breaches.

4.5. Assessment of a Breach

Does the breach relate to personal data?

Once it has been established that a breach has occurred, it must be ascertained what the nature of the breach is and whether the breach relates to personal data. If the breach does not relate to personal data then this must be catalogued and the basis of the assertion outlined in writing.

Should the breach relate to personal data, the categories of data which are involved must be set out in writing and it must be ascertained whether this relates to 'sensitive' categories of personal data also.

What is the exposure of the data subject?

The nature of the breach must be clarified in detail with respect the amount of exposure that the data subject has. Depending on the circumstances, it may be that there is high exposure or no exposure at all.

For instance, should a company laptop be stolen; if the laptop is neither password protected nor subject to encryption then it may be regarded as a high risk that the data contained on it may be exposed, however, if it is password protected, encrypted, and can be deleted/wiped remotely then the risk is much less.

It must also be noted whether the data breach has meant that the data of the data subject has been transferred outside of the EU.

What is the timeline of the breach?

As there are strict timelines set out in data protection legislation in relation to the notification by a controller to the Data Protection Commission and the data subject affected, it is important that 50808 make a note of the manner by which the breach was identified and the time of the identification in order to ensure that the process of informing those who are relevant is completed in a timely fashion.

4.6. Notification of the Data Subject/Individual involved

No need to notify the data subject

There are certain situations which do not require notification. 50808 need not contact the data subject if the personal data concerned is deemed to be unintelligible, i.e. device storing the data is encrypted, or if for another reason it is determined that the rights and freedoms of the data subject are unlikely to be exposed.

Exemption from need to notify data subject under section 94 of the Data Protection Act 2018

The obligation to inform the data subject of a breach of their personal data where it can be argued that a breach would lead to

(a) The obstruction of official or legal inquiries, investigations or procedures,
(b) Prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties,
(c) Protecting public security,
(d) Protecting national security, or
(e) Protecting the rights and freedoms of other persons.

The decision to avail of any of the above a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests

of the data subject. If availing of this exemption, 50808, need to inform the data subject of;

(f) The exemption,
(g) Their right to contact the Data Protection Commission in relation to the matter,
(h) Their right to seek recourse through the courts in relation to the matter.

Should notification of the data breach lead to circumstances as outlined in (a)-(e), then f)-h) need not apply.

If 50808 do not notify the data subject or the Data Protection Commission of the breach, it is best practice to make a written note of the reason or reasons why this was not done at the time the decision was made. This note should be retained on file.

Notifying the Data Subject

When 50808 is under an obligation to inform the data subject of the data breach which has occurred. Any notification should set out the following information;

a) The nature of the data breach should be described, in clear and plain language,
b) The data subject should be given a description of the likely consequences of the personal data breach,
c) A description should be given of the measures taken or proposed to be taken by the controller to address the personal data breach, including any measures taken or proposed to be taken to mitigate its possible adverse effects should be stated, and
d) The name and contact details of the 50808 Data Protection Officer should be made clear to the individual in question.

If contacting the respective data subjects is found to involve 'disproportionate effort' 50808 shall notify the data subjects concerned of the personal data breach by way of public communication or other similar measure that ensures the data subjects are informed of the personal data breach in an equally effective manner.

4.7. Notifying the Data Protection Commission

No need to notify the Data Protection Commission

Where, given the context of the breach and the personal data involved there is no risk to the rights and freedoms of data subjects, then there may be no need to contact the Commission. This decision and the reasons surrounding same should be logged in writing by the Data Protection Officer.

Notifying the Commission

Where a personal data breach has occurred 50808 is under an obligation to inform the Data Protection Commission within 72 hours of the breach occurring. Where 50808 does not inform the Commission within 72 hours of knowing of a breach they will subsequently have to explain to the Commission the reason why they did not notify within this time period.

There is a form to be found on the website of the Data Protection Commission for the notification of data breaches. If 50808 decide not to use this form, at least the notification to the Commission should outline the following information

(a) A description of the personal data breach, including, where possible the categories and number, or approximate number, of—

(i) data subjects concerned, and
(ii) personal data records concerned,

(b) A description of the likely consequences of the personal data breach, including whether the breach involved a cross border transfer of personal data,

(c) A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including any measures taken or proposed to be taken to mitigate its possible adverse effects, and

(d) The name and contact details of the controller's data protection manager or other point of contact.

Where it is not possible to outline the above information, any reason that this is not possible should be expressed in the notification and when the information does become available then it should be forwarded on to the Commission without undue delay.

Notification of a breach to the Data Protection Commission should be sent to breaches@dataprotection.ie.

4.8. Post-breach actions

50808 Data Protection Officer shall conduct a review of the data breach, the circumstances which lead to it, the effects of the breach on data subjects and shall outline any actions to be taken in order to mitigate future breaches. This should all be outlined in a report which may be sought at a future date by the Data Protection Commission.

4.9. Data Breach Checklist

a) Has the breach been assessed?

b) Have the Data Subject been notified?

c) Has the Data Protection Commission been notified?

d) Has the post-breach report been compiled?

Section 5: Data Subject Access Request Policy & Procedure

This policy is relevant to the spunout (Community Creations CLG) service 50808. Community Creations is undergoing a rebrand which will result in a name change to spunout. Once the legal name change has taken place this policy will be updated. 50808 and spunout.ie are currently trading names of Community Creations CLG.

5.1. Introduction

Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. These procedures provide a framework for responding to requests to exercise those rights. It is our policy to

ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law.

This policy should be read in conjunction with the 50808 privacy policies. Conflicts between the contents of this Policy and any other policies, processes or Data Protection Law should be notified to the Data Protection Officer ("DPO"). To the extent that there are inconsistencies between this Policy and Relevant Legislation, then the Relevant Legislation shall prevail, and this Policy shall be construed accordingly.

These procedures only apply to data subjects whose personal data we process.

5.2. Definitions

For the purposes of these procedures, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. Personal data relates to an identified or identifiable individual where the information, by reason of its content purpose or effect is linked to a person. It should be stressed that the data need not identify or describe an individual for it be personal data relating to that individual. If you are in doubt, please contact the Data Protection Officer on property.

"Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

Further definitions may be found in the 50808 data protection policy.

5.3 The Rights of the Individual/Data Subject

Where a data controller is processing or controls the processing of data of an individual, under Article 15 of the General Data Protection Regulation (GDPR) and s.91 of the Data Protection Act 2018 the individual has the right to

a. A description of;

i. The purposes of the processing;
ii. The categories of personal data concerned;
iii. The recipients of their personal data and whether these are located in outside the EU or in international organisations;
iv. The envisaged period of storage or where not possible the criteria which determine length of storage;

b. Request from the controller rectification, portability or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

c. Lodge a complaint with the Data Protection Commission;

d. A copy of the data concerned;

e. Any available information as to the source of the data where the personal data has not been collected from the data subject;

f. The existence of automated decision-making of their personal data, including profiling.

5.4. Logging the Request

A Subject Access request can be made to any staff member. Therefore, staff members are obliged to log the request for access and communicate this by email to the Data Protection Officer as soon as possible. Any wilful or negligent actions by employees in this process could lead to criminal conviction and internal disciplinary actions.

5.5. Identification/Verification

To comply with the law, information relating to the data subject must only be disclosed to that person or someone authorised to receive it on their behalf. For that reason, identity check for the individual must be completed, or the authority of the individual's representative should be established.

The following individuals are able to apply for access to personal data records:

a) The data subject to whom the personal data relates
b) The data subject's representative, with the data subject's consent
c) A person appointed by the Court
d) Relevant professional bodies
e) Law enforcement agencies

Upon verification of ID prior to processing the Subject Access Request, the requestor should be contacted in order to outline the proposed manner of response and the expected time in which this response shall be made.

Additional details should be sought which may aid the location of the relevant documents for instance;

a) work reference ID, or transaction reference ID

b) Alleged dates of processing
c) Manner/context of alleged processing
d) nature of the personal data allegedly being held
e) Relevant Phone number/Phone Bill

Requests from an individual

The individual may be known to the Data Protection Officer, however If the data subject has made the request themselves, one or a combination of the following can be sought in order to verify identity of the data subject;

a) Copy of a household bill in the name of the requestor
b) Copy of driver's licence.
c) Information about payment method on account
d) Information about most recent delivery

In the case of a texter requesting a copy of their personal data, to include the content of the conversations had using the services provided by 50808. In order to mitigate against any safeguarding issues which may apply, the SAR should be verified by the following steps:

a) A text message from the phone number, subject of the SAR, with the text 'SAR';
b) A copy of the relevant phone bill related to that number.

In the case of a texter requesting their personal data be erased, to include the content of the conversations had using the services provided by 50808. In order to mitigate against any safeguarding issues which may apply, the SAR should be verified by the following steps:

c) A text message from the phone number, subject of the SAR, with the text 'ERASE DATA';
d) A copy of the relevant phone bill related to that number.

In all cases the verification information provided should be recorded but the documentation containing personal data should be securely disposed of once the verification process has been completed.

Requests on an individuals' behalf or by parties other than the individual

Should someone be completing a request on behalf of a Data Subject then the basis on which they are making this request should be established. In the case of a Solicitor representing an individual, then a written authority may be sought in order to verify that 50808 may send relevant information to them in respect of the DSAR.

In other cases, the legal basis upon which the data is sought must be established, should that be court order/warrant etc where a copy of the original should be produced by the relevant parties.

5.6. Roles and Responsibilities of 50808 Staff Members

Members of Staff

Staff members must be aware of this policy and their obligations in relation to any data subject access request that they may receive in the course of their work.

Staff members must, on the direction of the DPO or any relevant data steward, carry out functions in relation to the compiling of a response to a Data Subject Access Request.

Board

The Board must support the DPO in their function in responding to a DSAR.

The Board must support the DPO in implementation of recommendations.

DPO

The DPO must advise relevant data stewards or staff members in relation to the creation of a response to a Data Subject Access Request.

The DPO must inform each member of staff in relation to procedure in reacting to a DSAR and obligation to notify DPO of the request.

The DPO must report to board in relation to the DSAR and the tasks undertaken when complying with same and any recommendations which may be applied when responding to a DSAR in the future.

The DPO must ensure that any recommendations which apply to staff are implemented.

5.7. Responding to Requests

Data Subject Access Request

Data subjects have the right to request access to their personal data processed by us. Unless there is an exemption that applies (see paragraph *Exemptions* below), we shall provide the data subject with a copy of the personal data processed by us within **one**

month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

Once all records relating to the data subject have been found, then two copies or prints of all should be made. 50808, should take one of the two copies of documents related to the requestor and apply any redactions that are necessary with reference to *Exemptions*, see below.

a) The reason for the redactions should be clearly stated i.e. 'third party personal data'.

b) Any documents that are to be with-held in their entirety should be listed and the reason for same should be outlined also.

c) Any codes or abbreviations within the documentation should be listed also in order for the requestor to fully understand the nature of the documentation.

A copy of the file as sent should be kept by 50808 in the same place as the copy of the documentation which has been compiled without redaction. Therefore, there are 3 copies of the requestors data as follows;

a) A copy of all data held by 50808 without redaction
b) A copy of all data held by 50808, with redactions applied
c) A copy of all data held by 50808, with redactions applied, sent to requestor

If the DSAR is manifestly unfounded or excessive, for example, because of its repetitive character, 50808 may charge a reasonable fee, considering the administrative costs of providing the personal data, or refuse to act on the request. The requestor shall be informed in writing, outlining any charges that will apply, should 50808 feel that this is the appropriate action to take.

If we are not going to respond to the DSAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the DPC.

A data subject may make a second request for data after the first. In this instance, should there be a short time period between both requests, only data which has been processed since the first request need be sent on in response to the second.

There is no set legislative period for 50808 to retain documents in relation to Data Protection Requests. Retaining the data for a period of 2 years post-reply may suffice

unless other circumstances determine otherwise such as the completion of legal proceedings.

Responding to requests to rectify personal data

Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall, unless there is an exemption (see paragraph Exemptions below), rectify the personal data without undue delay.

We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, our third-party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

Responding to requests for the erasure of personal data

Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see *Exemptions* below), erase the personal data without undue delay if:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;
c) the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;
d) the data subject objects to the processing of their personal data for direct marketing purposes;
e) the personal data have been unlawfully processed;
f) the personal data have to be erased for compliance with a legal obligation to which we are subject; or
g) the personal data have been collected in relation to the offer of e-commerce or other online services.

When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see *Exemptions* below), take the following steps:

a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this;
c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;
d) where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and
e) communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

If we are not going to respond to the request, we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the DPC.

In addition to the exemptions in paragraph *Exemptions* below, we can also refuse to erase the personal data to the extent processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;
c) for reasons of public interest in the area of public health;

d) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claims.

Responding to requests to restrict the processing of personal data

Data subjects have the right, unless there is an exemption (see paragraph Exemptions below), to restrict the processing of their personal data if:

a) the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;
b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and
d) the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

Where processing has been restricted, we shall only process the personal data (excluding storing them):

a) with the data subject's consent;
b) for the establishment, exercise or defence of legal claims;
c) for the protection of the rights of another person; or
d) for reasons of important public interest.

Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

Responding to requests for the portability of personal data

Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, we shall, unless there is an exemption (see paragraph *Exemptions* below), provide the personal data without undue delay if:

a) the legal basis for the processing of the personal data is consent or pursuant to a contract; and
b) our processing of those data is automated.

When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps:

a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity *see above*; and
c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period of response, we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

If we are not going to respond to the request, we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the DPC.

Responding to objections to the processing of personal data

Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either:

can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or are processing the personal data for the establishment, exercise or defence of legal claims. Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is

necessary for the performance of a task carried out for reasons of public interest.

Where such an objection is made, we shall, unless there is an exemption (see paragraph *Exemptions* below), no longer process a data subject's personal data.

Where personal data are processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

Responding to requests not to be subject to automated decision-making

Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see *Exemptions* below), no longer make such a decision unless it:

a) is necessary for entering into, or the performance of, a contract between us and the data subject;
b) is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.

If the decision falls within a) or c), we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

5.8. Exemptions

Data Protection Law provides that 50808 do not have to give a data subject all their data upon request. This is due to what are called 'exemptions', which means that all or some of a document may be with-held for a reason as is outlined in Data Protection Law. Exemptions may apply where it is necessary and proportionate in order to protect the following:

a) to safeguard cabinet confidentiality, parliamentary privilege, public or national security, defence, judicial independence and the international relations of the State;

b) for the purposes of carrying out any legal enquiries, investigations or procedures *and/or* for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties;
c) To protect the rights and freedoms, life and or safety of any person;
d) for the administration of any tax, duty or other money due or owing to the State or a local authority in any case in which the non-application of the restrictions concerned would be likely to prejudice the aforementioned administration;
e) to protect any third-party personal data;
f) to retain the confidentiality of any 'confidential expressions of opinion';
g) to retain confidentiality should the data consist of an estimate or estimation of liability in respect of a claim;
h) in the taking of, defence of or enforcement of any legal claim or to protect any legal Professional Privilege;
i) Data for the purposes of statistical or research purposes in the public interest.

If a document contains data which includes an exemption, then it may be suitable to redact either some or all of the document before sending it to the data subject in that form.

Many exemptions relate to matters such as national security or the independence of the judiciary which will not apply to the work of 50808. Here is a brief summation of the most relevant;

a) Third Party Personal Data

A data subject or individual is only allowed to seek data in relation to themselves. Where another person may be identifiable from a document relating to the requestor, any information which may identify the third-party data should be redacted unless the third party has given consent.

b) Confidential Expression of Opinion

Where a confidential opinion is expressed about the requestor by a member of staff this exemption may be relied upon however the bar in relation to what may be regarded as 'confidential' is set quite high, meaning it should not be presumed that all expressions of opinion are exempt.

c) Prejudice the prevention, detection or investigation of a criminal offence

If there is an allegation being made against an individual and it is felt that the disclosure of data in the context of the request could in some way hinder the

investigation then this exemption may be relied upon. However, once an investigation has been concluded, the exemption no longer applies.

d) Estimates

Should there be an estimate of liability in relation to a member or an employee with regard to a legal action or insurance claim this estimate need not be disclosed to the data subject.

e) Legal Professional privilege

Should documents be exempt from disclosure in court proceedings then the same applies in relation to a Subject Access Request, this applies to both legal advice and litigation privilege.

Further restrictions may be provided for in regulations under section 60(5) of the Data Protection Act 2018.

5.9 Data Subject Access Request Checklist

a) Has the date the request was received been logged?
b) ID/Verification
c) Initial response made to requestor
d) Documentation compiled
e) Exemptions and redactions applied
f) Copies of response and un-redacted documentation filed
g) Response sent
h) Retention period expired