Information Governance and GDPR Policy

Last Reviewed: 21st March 2024

The Queen's Award for Voluntary Service

1. Policy Statement of Intent

RammyMen provides services to a wide range of people, including adults and children who are extremely vulnerable and likely to share confidential and extremely sensitive details about themselves and about others.

It is the responsibility of everyone involved with RammyMen to ensure that all information is held and dealt with in a secure, responsible, considerate and legal manner.

The aim of this policy is to ensure that RammyMen and its personnel act appropriately and within the law with regard to information governance and the General Data Protection Regulation. It provides a framework to ensure that the organisation not only meets its legal requirements, but also treats information and data with the high standard of care expected by everyone involved with RammyMen.

This policy will be reviewed regularly and revised as appropriate under the guidance of the designated Data Protection Officer / Data Controller / Information Governance Lead (hereinafter called 'Data Controller' in line with the Data Protection Act 2018 nomenclature) and by a Data Quality Forum.

Rob Moss
62 Stubbins St
Ramsbottom
BL0 0NL
rob@rmdirect.org
07944 038512

2. Collection of Data

2.1 All collection and processing of personal data shall be lawful and fair and carried out in line with the Data Protection Act 2018.

2.2 All personal data shall be obtained with the data subject's consent, or that of a responsible adult in the case of a child, except where such data is sought and required for the protection and safety of staff, volunteers and/or members of the organisation. These exceptions will apply where an attendee's criminal or mental health history need particular safeguarding attention.

2.3 Where data is received from referral agencies, it shall be on the understanding that they have obtained, processed and forwarded that data in line with the Data Protection Act 2018 in conjunction with the GDPR.

2.4 All initial referal forms shall by default contain the clause: "I confirm that I have sought the client or patient's permission to pass on the above information."

2.5 Where data is submitted by a person, there shall be no ambiguity about the reasons for that data to be collected and its use by the organisation. That data shall not be used for any reason other than those communicated to the person unless further authorisation for that specific use is obtained. Any data use permissions sought shall be recorded along with the personal data itself.

2.6 Personal data submitted by web-based form shall be server-side encrypted using 256-bit encryption before being forwarded to protonmail.me in order that it may not be intercepted in a useable form.

2.7 Only data that is necessary for the performance of the stated purposes shall be collected, stored and processed.

2.8 There shall be no collection of "sensitive data" such as racial or ethnic origin, political opinions, religious or philosophical beliefs, gender identity, sexual preference or trade union membership unless being carried out specifically as part of a study into those characteristics.

2.9 The date that an individual last communicated or otherwise engaged with the organisation shall be stored alongside their personal data so that the accuracy of held data may be assessed, and historical data dealt with as detailed in section 4.

2.10 Websites and other online resources shall not collect or store any personally-identifiable data on a subject whether through cookies, beacons, web-analytics or similar.

2.11 Any data collection activities shall be discussed with the Data Controller before being initiated, and plans made for collection method, data use, length of storage, permissions for use, methods of storage, storage security and destruction. Any risks shall be identified, and procedures put in place for data processing in line with this policy document.

2.12 If data is collected on an individual under the age of 18 then this shall be explicitly noted with a date of birth if data may be held for a significant length of time.

3. Storage of Data

3.1 Organisational email addresses shall be created and operated using protonmail.me which is end-to-end encrypted with zero-access and AES, RSA and OpenPGP encryption. A local client shall not be installed, with all email data held on the server and no local copies of sensitive personally-identifiable data made.

3.2 Any personal data which needs to be stored outside of protonmail.me shall be stored on a strong-password protected AES-256 (minimum) encrypted drive, with the vault regularly backed up to a second AES-256 (minimum) encrypted drive or RAID level 1 encrypted disk.

3.3 With the exception of encrypted email storage, all personal data shall be stored within the United Kingdom.

3.4 No personally identifable data shall be stored on any web-based system other than protonmail in the case of emails or organisational bank account transaction information. This includes online server databases, even in encrypted form.

3.5 Every reasonable step shall be taken to ensure that personal data is accurate and up-to-date.

3.6 Personal data based on facts shall be distinctly identified from data based on personal assessments.

4. Destruction of Data

4.1 Data may only be held for such time as is appropriate based on original permissions sought. These limits shall be:

- Until informed of an individual's disinterest in receiving further communications in the case of a 'keep us updated' or newsletter subscription
- Until the data is no longer of relevance for the original permissions, unless new permissions are sought

4.2 Data may only be held for six months after its permitted use has expired. It shall then be removed from current databases and dealt with as detailed elsewhere in section 4. Periodic reviews of retained information shall be carried out in order to identify affected data.

4.3 Any individual who has not reciprocated communications from the organisation within five years shall be deemed 'inactive' and their data removed from current databases.

4.4 The choice of erasure or achiving of old data (with access restricted) shall be made on a case-by-case basis dependent upon historical safeguarding, insurance, reporting, litigation, statutory recording and health issues.

4.5 Upon learning that data is no longer accurate, that data shall be updated, archived or erased as appropriate.

5 Data Information Requests

5.1 In the case of a data information request for an NHS-commissioned service, the organisation shall not respond to that request, but shall instead transfer it to Penine Care CCG.

5.2 An individual may submit a Subject Access Request for data held on them verbally or in writing. A Subject Access Form is appended to this policy and is the prefered method. The data shall be securely communicated within one month.

5.3 If a child submits a Subject Access Request and is considered mature enough to understand their rights then the child shall be responded to directly. Otherwise the child will be encouraged to involve a responsible adult in the request.

5.4 If there is any doubt as to the identity of someone submitting a Subject Access Request then photographic ID shall be required before any request is considered. No information will be provided about the person (including whether or not they have engaged with the organisation) until the photographic ID has been verified.

5.5 The organisation exercises its right to refuse a Subject Access Request if it is considered to be excessive or unfounded. If this is the case then the individual must be informed of the reasons why, their right to make a complaint to the Information Commissioner's Office, their right to make a request to the Information Commissioner's Office and their right to apply to a court under section 167 of the Data Protection Act 2018.

5.6 There are some special cases and exemptions from Subject Access Request legislation, including health data, social work data, confidential references, negotiations, pending legal proceedings or criminal investigations and functions designed to protect the public. If any of these are pertinent then advice should be sought from the Data Controller and from the Information Commissioner's Office.

5.7 If the decision is taken to reject a Subject Access Request then the reasons shall be formally recorded in a format suitable for sharing with the Information Commissioner's Office if required.

5.8 If requested by a data subject, the organisation must rectify inaccurate or incomplete personal data without undue delay. If it is necessary for ongoing proceedings for historical data to be retained then a record shall be kept of the original data.

5.9 If any data received from other agencies or communicated to other agencies is identified as inaccurate then those agencies shall be informed.

5.10 Where a third party individual or organisation requests information regarding other individuals who have not provided consent for that use of their data, then that request for information will be rejected or data shall be supplied with all identifying information redacted.

6 Breaches of Data Security

6.1 If information has been legitimately shared but has subsequently been found to be innacurate, or information has been unlawfully shared then the recipient must be notified without delay.

6.2 If data is suspected of having been inappropriately accessed or shared then the Data Controller shall be immediately informed so that they may inform the Information Commissioner's Office and other appropriate authorities. Immediate action shall be taken to ensure further breaches are blocked.

6.3 Where a breach of data security is identified, a review of current security procedures and of this document shall be carried out with recommendations for improvements made.

6.4 If a personal data breach has been identified and is likely to result in a high risk to the rights and freedoms of individuals then the Data Controller must inform the data subject of the breach without undue delay.

7 Sharing of Data

7.1 Personal data shall only be communicated within the organisation as is required for the delivery of services in a safe and effective manner, and shall not be shared for any other reason.

7.2 Personal data shall not be communicated outside of the organisation unless consent is explicitly sought from the person or a responsible adult in the case of a child, or there is a criminal or safeguarding issue that mandates its communication. If in doubt, advice shall be sought from the Data Controller named on page 2.

7.3 Sensitive data (eg health, financial situation, marital difficulties, criminal records etc) shall only be shared where that data is crucial to the provision of a service, and only to those individuals that have a direct need for that data and have received and read a copy of this policy.

7.4 Anonymised data may be shared for the means of reporting. However, where a person's situation is unique enough to render them easily identifiable, their permission to share their 'anonymised' data shall be sought.

7.5 Where a terrorism risk (threat to public security) or risk to the safety of another individual is suspected then RammyMen cannot guarantee that any data or information supplied will be held in confidence, or that the information will not be passed to the relevant authorities. Any information of this nature shall be immediately communicated to the Data Controller.

7.6 Any shared data shall be verified as currently accurate and up-to-date prior to being shared. Where accuracy cannot be confirmed, a date when the information was last known to be accurate shall be communicated.

8 Use of Data

8.1 Personal data may only be used for the purpose for which it was collected, and for which permission was provided. Any use beyond original permissions shall require further explicit permission to be sought unless required by law.

8.2 No personal data shall be used for any kind of automated procession (profiling) unless it has been completely anonymised.

8.3 Only people who have been provided with, read and signed a copy of this policy shall be permitted access to any personal data.

8.4 Records shall be kept of all people designated data access and their roles and access levels.

9 Safety of Data

9.1 All encryption and email passwords shall be 'strong' with no use of 'dictionary' words, the inclusion of numbers and 'special characters' such as !"@:£. Use of names, adjacent keys on the keyboard and common substitutions such as 4 in place of a or 0 in place of o shall be discouraged.

10 Transparency of Information Governance and GDPR

10.1 This document shall be made available on the organisation website and shall be available in printed form to anyone who requests a copy.

11 Roles of the Data Controller

11.1 The Data Controller shall ensure that the organisation complies with the Data Protection Act 2018 legally and within the spirit of the act and the six data protection principles.

11.2 The Data Controller shall ensure that this policy document is adhered to consistently and completely.

11.3 The Data Controller shall handle all Subject Access Requests.

11.4 The Data Controller shall maintain a log of all issues, breaches, data officer roles, Subject Access Requests and any other information required by this policy.

11.5 The Data Controller shall maintain and manage the periodic review of this document.

11.6 The Data Controller shall ensure the organisation meets its obligations in relation to the Information Commissioner's Office.

11.7 Where a type of data processing is likely to carry a significant risk, the Data Controller is responsible for instigating and carrying out a Data Protection Impact Assessment in line with the Information Commissioner's Office guidelines.

11.8 In the case of a personal data breach, the Data Controller is responsible for informing the Information Commissioner's Office not later than 72 hours after becoming aware of it, including all data required under section 67 of the Data Protection Act 2018.

13. GDPR Checklists

The following checklists are taken from the Information Commissioner's Office publication - Guide to the General Data Protection Regulation (GDPR) and shall be used as a guide.

Lawful Basis for Processing

☐ We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.

☐ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.

☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.

☐ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

☐ Where we process special category data, we have also identified a condition for processing special category data, and have documented this.

☐ Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

Asking for Consent

☐ We have checked that consent is the most appropriate lawful basis for processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask people to positively opt in.

☐ We don't use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we're going to do with it.

☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

☐ We name our organisation and any third party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording Consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Managing Consent

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don't penalise individuals who wish to withdraw consent.

Legitimate Interests

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual's interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.

☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children's data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review, and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy information.

Right to be Informed

What to provide

We provide individuals with all the following privacy information:

☐ The name and contact details of our organisation.

☐ The name and contact details of our representative (if applicable).

☐ The contact details of our data protection officer (if applicable).

☐ The purposes of the processing.

☐ The lawful basis for the processing.

☐ The legitimate interests for the processing (if applicable).

☐ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

☐ The recipients or categories of recipients of the personal data.

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

☐ The retention periods for the personal data.

☐ The rights available to individuals in respect of the processing.

☐ The right to withdraw consent (if applicable).

☐ The right to lodge a complaint with a supervisory authority.

☐ The source of the personal data (if the personal data is not obtained from the individual it relates to).

☐ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

☐ The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

☐ We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- ☐ within a reasonable of period of obtaining the personal data and no later than one month;
- ☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- ☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

- ☐ concise;
- ☐ transparent;
- ☐ intelligible;
- ☐ easily accessible; and
- ☐ uses clear and plain language.

Changes to the information

☐ We regularly review and, where necessary, update our privacy information.

☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

☐ We undertake an information audit to find out what personal data we hold and what we do with it.

☐ We put ourselves in the position of the people we're collecting information about.

☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

☐ a layered approach;

☐ dashboards;

☐ just-in-time notices;

☐ icons; and

☐ mobile and smart device functionalities.

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from other sources
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓

The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

Right of Access

Preparing for subject access requests

☐ We know how to recognise a subject access request and we understand when the right of access applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

☐ We understand the nature of the supplementary information we need to provide in response to a subject access request.

Complying with subject access requests

☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.

☐ We understand what we need to consider if a request includes information about others.

Right To Rectification

☐ We know how to recognise a request for rectification and we understand when this right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for rectification

☐ We have processes in place to ensure that we respond to a request for rectification without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We have appropriate systems to rectify or complete information, or provide a supplementary statement.

☐ We have procedures in place to inform any recipients if we rectify any data we have shared with them.

Right to Erasure

☐ We know how to recognise a request for erasure and we understand when the right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for erasure

☐ We have processes in place to ensure that we respond to a request for erasure without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.

☐ We have procedures in place to inform any recipients if we erase any data we have shared with them.

☐ We have appropriate methods in place to erase information.

Right to Restrict Processing

☐ We know how to recognise a request for restriction and we understand when the right applies.

☐ We have a policy in place for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for restriction

☐ We have processes in place to ensure that we respond to a request for restriction without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

☐ We have appropriate methods in place to restrict the processing of personal data on our systems.

☐ We have appropriate methods in place to indicate on our systems that further processing has been restricted.

☐ We understand the circumstances when we can process personal data that has been restricted.

☐ We have procedures in place to inform any recipients if we restrict any data we have shared with them.

☐ We understand that we need to tell individuals before we lift a restriction on processing.

Right to Data Portability

☐ We know how to recognise a request for data portability and we understand when the right applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

Complying with requests for data portability

☐ We can transmit personal data in structured, commonly used and machine readable formats.

☐ We use secure methods to transmit personal data.

☐ We have processes in place to ensure that we respond to a request for data portability without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to a request.

Right to Object

☐ We know how to recognise an objection and we understand when the right applies.

☐ We have a policy in place for how to record objections we receive verbally.

☐ We understand when we can refuse an objection and are aware of the information we need to provide to individuals when we do so.

☐ We have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights.

☐ We understand when we need to inform individuals of their right to object in addition to including it in our privacy notice.

Complying with requests which object to processing

☐ We have processes in place to ensure that we respond to an objection without undue delay and within one month of receipt.

☐ We are aware of the circumstances when we can extend the time limit to respond to an objection.

☐ We have appropriate methods in place to erase, suppress or otherwise cease processing personal data.

Data Protection Impact Assessments

DPIA awareness checklist

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

☐ We always carry out a DPIA if we plan to:

- ☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- ☐ Process special category data or criminal offence data on a large scale.
- ☐ Systematically monitor a publicly accessible place on a large scale.
- ☐ Use new technologies.
- ☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- ☐ Carry out profiling on a large scale.
- ☐ Process biometric or genetic data.
- ☐ Combine, compare or match data from multiple sources.
- ☐ Process personal data without providing a privacy notice directly to the individual.
- ☐ Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- ☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- ☐ Process personal data which could result in a risk of physical harm in the event of a security breach.

☐ We consider whether to do a DPIA if we plan to carry out any other:

- ☐ Evaluation or scoring.
- ☐ Automated decision-making with significant effects.
- ☐ Systematic
- ☐ Processing of sensitive data or data of a highly personal nature.
- ☐ Processing on a large scale.
- ☐ Processing of data concerning vulnerable data subjects.
- ☐ Innovative technological or organisational solutions.
- ☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ If we decide not to carry out a DPIA, we document our reasons.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.

☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures we identified, and integrate them into our project plan.

☐ We consult the ICO before processing, if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them when necessary.

Security

☐ We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.

☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.

☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.

☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

☐ We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.

☐ We use encryption and/or pseudonymisation where it is appropriate to do so.

☐ We understand the requirements of confidentiality, integrity and availability for the personal data we process.

☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

☐ We ensure that any data processor we use also implements appropriate technical and organisational measures.

Personal Data Breaches

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We have a process to inform affected individuals about a breach when it is likely to result in a

high risk to their rights and freedoms.

☐ We know we must inform affected individuals without undue delay.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.

Children

General

☐ We comply with all the requirements of the GDPR, not just those specifically relating to children and included in this checklist.

☐ We design our processing with children in mind from the outset, and use a data protection by design and by default approach.

☐ We make sure that our processing is fair and complies with the data protection principles.

☐ As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to children.

☐ If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.

☐ As a matter of good practice, we consult with children as appropriate when designing our processing.

Bases for processing a child's personal data

☐ When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance in power in the relationship between us.

☐ When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.

☐ When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Offering an information Society Service (ISS) directly to a child, on the basis of consent

☐ If we decide not to offer our ISS (online service) directly to children, then we mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.

☐ When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.

☐ When offering ISS to UK children on the basis of consent, we obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.

☐ When targeting wider European markets we comply with the age limits applicable in each Member state.

☐ We regularly review available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.

☐ We don't seek parental consent when offering online preventive or counselling services to a child.

Marketing

☐ When considering marketing children we take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.

☐ We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.

☐ We stop processing a child's personal data for the purposes of direct marketing if they ask us to.

☐ We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).

Privacy notices

☐ Our privacy notices are clear, and written in plain, age-appropriate language.

☐ We use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.

☐ We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.

☐ As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

☐ We tell children what rights they have over their personal data in language they can understand.

☐ As a matter of good practice, if we are relying upon parental consent then we offer two different versions of our privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

☐ We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.

☐ We allow competent children to exercise their own data protection rights.

☐ If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.

☐ We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

The Child's Data Protection Rights

☐ We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.

☐ We allow competent children to exercise their own data protection rights.

☐ If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.

☐ We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

Subject Access Request Form

Please complete this form to access a copy of the data held about yourself or someone who is under your care. Please be aware that we may need to see photographic Id in order to protect individuals' privacy. RammyMen imposes no charge for Subject Access Requests.

Name of person completing the form :

Date of Request :

Address of person completing the form:

Name of person whose data is requested :

Relationship between the above people (if different) :

Any specific information requested :

For office use only:
Date request received :
Id and relationship to subject confirmed? (please sign) :