MERRYWOOD PRACTICE

Individual Rights under the Data Protection and Access to Health Records Act

Standard Operating Procedure

The Merrywood Practice
January 2019

Contents

1. Introduction and Purpose

The purpose of this standard operating procedure (SOP) is to provide detailed guidance on how to process Individual's Rights requests under the General Data Protection Regulation (GDPR) 2016 and Data Protection Act (DPA) 2018 (commonly referred to as the Data Protection Legislation).

Requests made under this legislation only relate to living individuals. The SOP will also cover requests received under the Access to Health Records Act (AHRA) 1990 which specifically relates to deceased individuals.

This SOP is designed to act as supplementary guidance to the organisations Individual Rights Policy. **The SOP must be read in conjunction with the policy**.

2. Scope and Definitions

The SOP will cover the following GDPR and DPA rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

This SOP will also cover the rights of access to personal data for deceased individuals under the AHRA.

The SOP will provide detailed guidance on when each of the rights are available and provide procedural guidance on how to process each type of request.

All organisations that hold personal data or special categories of data are duty bound under the Data Protection Legislation and AHRA to comply with the above rights/requests.

This SOP is intended for all staff but particularly for staff who are responsible for processing Individuals Rights requests as well as any other staff whose role specifically requires them to manage requests of this nature.

It is essential that all staff responsible for such requests read, understand and follow this SOP.

The definitions are included in the Individual Rights Policy.

3. Roles and Responsibilities

The responsibilities are included in the Individual Rights Policy.

4. Specific Procedures

RIGHT TO BE INFORMED	FAIR PROCESSING NOTICE
RIGHT OF ACCESS	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED DECEASED INDIVIDUALS – DEALT WITH UNDER AHRA 1990 IN FAIR PROCESSING NOTICE APPLIES IN ALL CIRCUMSTANCES CAPACITY AND REPRESENTATIVES EXEMPTIONS APPLY NO CHARGE
RIGHT TO RECTIFICATION	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES EXEMPTIONS APPLY NO CHARGE
RIGHT TO ERASURE	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES EXEMPTIONS APPLY NO CHARGE
RIGHT TO RESTRICT PROCESSING	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE APPLIES IN ALL CIRCUMSTANCES EXEMPTIONS DO NOT APPLY NO CHARGE
RIGHT TO DATA PORTABILITY	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES EXEMPTIONS DO NOT APPLY NO CHARGE
RIGHT TO OBJECT	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES SOME EXEMPTIONS APPLY NO CHARGE
RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION MAKING	VERBAL OR IN WRITING 28 DAYS TO COMPLETE ID REQUIRED IN FAIR PROCESSING NOTICE DOES NOT APPLY IN ALL CIRCUMSTANCES SOME EXEMPTIONS APPLY NO CHARGE

Right to Be Informed (Article 12-14)

Individuals have the right to be informed about the collection and use of their personal data under Article 12-14 of the GDPR. This is a key transparency requirement under the GDPR. We are obliged to provide individuals with information including, the purposes of processing an individual's personal data, the retention periods for that personal data and whether it will be shared with anyone else. This detail can be found in the organisations Fair Processing Notice (or Privacy Notice). The Individuals' Rights policy provides sufficient detail regarding this right and therefore needs no further explanation in this SOP. For further detail please see Appendix A in the policy.

Right of Access/Subject Access Request (Article 15)

Overview

The right of access, commonly referred to as subject access, gives individuals the right to have confirmation that their personal data is being processed, to obtain a copy of their personal data and other supplementary information. The information that must be provided largely corresponds with the information detailed in the organisations Fair Processing Notice.

Receiving a Request

The GDPR does not specify how to make a valid request. Therefore, an individual (or a third party acting on the individuals behalf) can make a request verbally or in writing. It can also be made to any part of the organisation (including by social media) and does not have to be to a specific person or contact point.

The request does not have to include the phrase 'subject access' 'right of access' or 'Article 15'. However a request must be for access to personal data (including special categories of personal data) relating to the individual and not to information relating to other people. If a request is received it must be immediately logged with the team/individual responsible for processing such requests. The request must be logged on the Practice's right of access/SAR log.

The GDPR does not require individuals to make a SAR using a particular form and this cannot be used as a means for extending the timescales for compliance in its own right; however it is good practice to provide a means for individuals to identify all relevant details that the organisation will/may require in locating the information.

Template letters and forms can be found at section 6 of the SOP.

Practice Staff can submit a request for access to their personal data to the Strategic Business Manager

Once a request is received it must be acknowledged without undue delay and at least within 48 hours of receipt into the organisation. The organisation has one calendar month to respond to a SAR, but an organisational decision has been taken to adopt a 28 day response time limit (in accordance with ICO guidance). Therefore all requests must be completed within 28 days of receipt. The timescale for responding may be extended by a further two months if the request is complex or if we have received a number of requests from an individual. However we must inform the individual within one month of receiving the request why the extension is necessary.

A request may be received for access to a deceased individual's personal data. This will not be dealt with under the rights offered by the GDPR. Please refer to the Access to Health Records section below.

Processing the Request

Once the request has been received and logged we must ensure that we are satisfied as to the identity of the individual making the request. The key is proportionality and we must only request enough information to confirm who they are. This must be requested without undue delay and at least within 48 hours of receipt of the request. The period for responding to the request begins once the ID has been received. Forms of ID which are acceptable:

Primary documents for proof of identity:	**Secondary documents for proof of identity**
• UK passport / other country passport • Driving Licence • Adoption certificate • Separation document • Annulment document • National ID card • NINO card with National Insurance Number • National Insurance contributions form • Medical card with NHS number Change of name document **Certified copies of documents** can be provided by: 1. Posting the original to us by recorded delivery 2. Bringing them into our offices for us to copy 3. Having the originals certified by an individual or organisation. For further details please visit the following website: Certifying-a-document	• Pay slip • Tenancy agreement, rent book or rent card • Utility bills such as gas, electricity and water • Fixed telephone bills • Railcard, travel card and bus-pass • Season ticket. • Bank or Building Society debit or credit cards • Store charge card • Bank or building society statement / passbook • Shares certificates • Life insurance policy • Trade Union membership card • State benefit Book/Notification letter • Sub-contractors certificate • P45 • EHIC – European Healthcare Insurance Card

If an individual makes a request electronically, the information should be provided in a commonly used electronic format, unless the individual requests otherwise.

A request under the right of access relates to the data held at the time the request is received. However, in many cases, routine use of the data may result in it being amended or even deleted while the request is being dealt with. Therefore it is reasonable to supply information that is held at the time the request is responded to, even if this is different to that held when the request was received. However, it is not acceptable to amend or delete the data if we would not otherwise have done so. Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

The GDPR requires that the information provided to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will be particularly important where the information is addressed to a child. Therefore the organisation may be required to explain particular references, acronyms or information which is provided to the individual.

If a request is received but more information is required in order to clarify the request this must be requested without undue delay. However we must only ask for information that is reasonably required to find the personal data covered by the request. The period for responding to the request begins once the additional information is received. However, if an individual refuses to provide any additional information, we must still endeavour to comply with the request i.e. by making reasonable searches for the information covered by the request.

Under the GDPR, in most cases a fee cannot be charged. However where the request is manifestly unfounded or excessive we may charge a "reasonable fee" for the administrative costs of complying with the request. We can also charge a reasonable fee if an individual requests further copies of their data following a request. The fee must be based on the administrative costs of providing further copies.

Requests Received From Representatives or Third Parties

The GDPR does not prevent an individual making a valid request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act on their behalf. In these cases, we must be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This may be in the form of a written consent/authority form evidencing that the third party has consent from the individual to access their personal data.

A Third Party Authorisation form (for a representative to complete) has been prepared for situations where this is necessary which can be found in section 6.

Guidance should be sought from the Caldicott Guardian and Data Protection Officer if there are any concerns over the nature of the information and whether there are concerns as to whether the data subject is aware of what might be shared with the representative.

Requests may also be received from those who hold power of attorney; if the individual lacks mental capacity. There are no specific provisions under the GDPR or Mental Capacity Act 2005 enabling a third party to exercise access rights on behalf of such an individual therefore it is reasonable to assume that an attorney with authority to manage the affairs of an individual (or under a deputyship order) will have the appropriate authority.

We will need to see evidence that the attorney holds a sealed power of attorney for health and welfare purposes (and in some circumstances for property and affairs) or a

deputyship order from the Court of Protection. ID will also need to be requested if we are unsure as to their identity (see above section).

The Lasting Power of Attorney (LPA) gives the attorney authority to make decisions on behalf of the person who has requested the LPA (known as the Donor) and the attorney has a duty to act or make decisions in the best interests of the person who has made the LPA.

There are two different types of LPA:

1. A personal welfare LPA is for decisions about both health and personal Welfare.
2. A property and affairs LPA is for decisions about financial matters.

There may be times when carrying out the duties as an Attorney that s/he needs to access personal information about the Donor, for example from a doctor, to help make a decision that is in the Donor's best interests. Most of this information will be personal information relating to the Donor and much of it will be sensitive and/or confidential.

Providing the attorney is acting within the powers given within the LPA, s/he is entitled to ask for this information in the same way the Donor would have done if they had the capacity to do so. The attorney is only entitled to the information that is necessary for the decision(s) that have to be made e.g. the past medical history that has no bearing on the issue at hand should not be revealed.

Seek advice from the Data Protection Officer if concerns arise about releasing information under a particular LPA.

A child has a right under the GDPR to have access to their personal data regardless of their age. However children under a particular age will likely have their rights exercised by those who have parental responsibility for them.

Therefore before responding to a request for information about a child we must consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should respond directly to the child, unless the child authorises their parent (or an individual with parental responsibility) to act on their behalf.

To determine whether the child is mature enough to understand their rights we must take into account the following:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

- any views the child or young person has on whether their parents should have access to information about them
- any views the child or young person has on whether their parents should have access to information about them

Children aged over 16 years are presumed to be competent. Children under 16 in England, Wales and Northern Ireland must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to an SAR. However, children who are aged 12 or over are generally expected to have the competence to give or withhold their consent to the release of information from their health records. In Scotland, anyone aged 12 or over is legally presumed to have such competence. When assessing a child's competence, it is important to explain the issues in a way that is suitable for their age. The Gillick competency test or Fraser guidelines can also be used to determine whether a child is presumed to be of a sufficient age/maturity.

For further information on situations where the request has been made by a child, see the ICO guidance on children and the GDPR .

Other Peoples' Information

Responding to an access request may involve providing information that relates both to the individual making the request and to another individual.

The Data Protection Act 2018 says that we do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, we must take into account all of the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual

So, although we may sometimes be able to disclose information relating to a third party, we need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, we must decide whether to disclose the information anyway.

For the avoidance of doubt, we cannot refuse to provide access to personal data about an individual simply because you obtained that data from a third party. The rules about third party data apply only to personal data which includes both information about the

individual who is the subject of the request and information about someone else. Good practice would be to redact information that relates to another individual.

Requests for Deceased Individual's Records

The Access to Health Records Act 1990 (AHRA) provides a small cohort of people with a statutory right to apply for access to information contained within a deceased person's health record.

There may be circumstances where individuals who do not have a statutory right of access under AHRA request access to a deceased patient's record. Current legal advice is that the Courts would accept that confidentiality obligations owed by health professionals continue after death. Each request should be reviewed on a case by case basis and advice should be sought from the Caldicott Guardian if there are any concerns regarding disclosing any personal information.

Individuals who have a right of access under the AHRA are defined under Section 3(1) (f) of the Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.

The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record.

There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the record holder should seek legal advice and speak to the Data Protection Officer.

There are different requirements to the GDPR/DPA in terms of timescales; Access to Health Records requests should be responded to within 40 calendar days and there can be no charge for the request. It is still a requirement to check the validity of the request (ID etc.). No prescribed form needs to be completed however we must be satisfied as to the identity of the individual making the request and we can therefore seek clarification from the requestor. If a request is received from a patient's personal representative evidence must be provided such as a sealed Grant of Probate or valid Will evidencing that the individual making the request is a personal representative. If the individual died intestate, the individual making the request can apply for Letters of Administration.

Disclosures in the absence of a statutory basis should be in the public interest, be proportionate, and judged on a case-by-case basis. The public good that would be served by disclosure must outweigh both the obligation of confidentiality owed to the deceased individual, any other individuals referenced in a record, and the overall importance placed in the health service providing a confidential service. Key issues for consideration include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following the disclosure, and any loss of privacy that might result and the impact upon the reputation of the deceased. The views

of surviving family and the length of time after death are also important considerations. The obligation of confidentiality to the deceased is likely to be less than that owed to living patients and will diminish over time.

Another important consideration is the extent of the disclosure. Disclosing a complete health record is likely to require a stronger justification than a partial disclosure of information abstracted from the record. If the point of interest is the latest clinical episode or cause of death, then disclosure, where this is judged appropriate, should be limited to the pertinent details.

If the deceased individual expressed a wish for information to remain confidential this should be upheld regardless of who is making the request unless there is an overriding public interest in disclosing.

For further guidance, please refer to the NHS Choices deceased individuals records.

Refusing to Comply With a Request
If we consider that a request is 'manifestly unfounded' or excessive we can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request

In either case we will need to justify the decision. For further advice please contact the Data Protection Officer.

If we do refuse to comply with a request we must explain the reasons we are not taking action; advise the individual of their right to make a complaint to the ICO and their ability to seek to enforce a right through a judicial remedy. The ICOs address is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Exemptions
There are a number of exemptions from the individual rights under the GDPR. The relevant exemptions have been detailed below.

Information required to be disclosed by law etc or in connection with legal proceedings
Schedule 2, Part 1, paragraph 5 of the DPA 2018 provides an exemption when Information is required to be disclosed by law etc or in connection with legal proceedings. The listed GDPR provisions (in Schedule 2, Part 1, paragraph 1) do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public

Crime and Taxation

Schedule 2, Part 1, paragraph 2 of the DPA 2018 provides an exemption for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of tax or duty from Articles 13-18 and 20-22, which includes the right of access provisions. Therefore if information is requested by a competent authority such as the Police, personal data can be disclosed without the consent of the data subject if the conditions in Schedule 1, Part 1, paragraph 10 are met i.e for the purposes of the prevention or detection of an unlawful act.

Legal Professional Privilege

Under Schedule 2, Part 4, paragraph 19 of the DPA 2018, information that relates to legal professional privilege is exempt from the right of access and duty to be informed provisions (Article 15, 13 and 14) of the GDPR.

Confidential References

Under Schedule 2, Part 4, paragraph 24 of the DPA 2018 confidential references (those references given in confidence) are exempt from the right of access provision (Article 15) as well as the duty to be informed under Article 13 and 14 of the GDPR if the personal data consists of a confidential reference for the purposes of including the education, training or employment of the data subject. This exemption also applies to the appointment of the data subject to any office, including that of a volunteer, or the provision of any service by the data subject.

Health data processed by a Court

Schedule 3, Part 1, paragraph 3 of the DPA 2018 states that the rights under Articles 13, 14, 15, 16, 17, 18, 20, 21 and Article 5 (General Principles) of the GDPR do not apply where health data is processed by a court, is contained in a report or other evidence under proceedings and rules detailed in the Data Protection Act 2018 or the data can be withheld in whole or in part from the data subject by the Court;

Requests made by others

Under Schedule 3, Part 1, paragraph 4 (1) (a), where the data subject is an individual aged under 18 and the person making the request has parental responsibility for the data subject or (1) (c) where the data subject is incapable of managing his or her own affairs and a Court appointed representative is managing their affairs, the rights under Articles 13, 14, 15, 16, 17, 18, 20, 21 and Article 5 (General Principles) do not apply concerning health data where to comply with that request would

(a) release data given by the data subject in the expectation that it would not be shared with the person making the request on their behalf or;
(b) release the results of an examination or investigation carried out under the data subjects consent with the understanding that the result would NOT be disclosed or;
(c) release information that the data subject has expressly indicated should not be disclosed;

Serious harm from health data disclosure

Under Schedule 3, Part 1, paragraph 5 of the DPA 2018 health records may be withheld from disclosure under Article 15(1) and (3) of the GDPR when the serious harm test is met or where a controller who is not a health professional obtains an opinion from someone who appears to be an appropriate health professional. The "serious harm test" involves consideration of whether the application of the Article 15 Right of Access to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual. However, the opinion of the Health Professional will not be relevant if it was obtained prior to a period of 6 months before the request or, it is felt that it would be advisable to re-check that opinion;

Information already known by the Data Subject

Under Schedule 3, Part 1, paragraph 6 of the DPA 2018 an exemption cannot be applied to a request under Article 15 where it is apparent that the data subject has already seen or knows about the health information;

Disclosure of Records

Before supplying any information in response to a request, please check that we have the requester's correct postal or email address (or both) – whichever the requestor has asked for the information to be sent by. If sending paper copies, ensure the information is sent via Royal Mail Special Delivery. If the requestor chooses to collect the information; ID must be checked and the requestor must sign a collection receipt.

The DPA/GDPR requires that the information you supply to the individual is in intelligible form. At its most basic, this means the information should be understandable by the average person. Therefore all records must contain explanations of codes or abbreviations where appropriate. Do not provide original records, only photocopies.

If information has been withheld due to an exemption, for example, information relating to another individual, legal privilege etc. – this must be documented on the Individuals Rights Log (including justification for applying the exemption) and explained to the requestor that information has been redacted/removed in accordance with the provisions set out in the GDPR/DPA.

The requestor may ask for the information to be disclosed to them over e-mail. If this is the case, we must explain to the individual that the information will not be transmitted with encryption and therefore we cannot guarantee that the information will be sent securely. The individual will need to confirm that they understand this and agree for the information to be sent electronically (e.g. by confirming agreement in response to the email).

Please remember to keep a copy of the information disclosed.

Retention

The log and all documentation relating to a particular request should be kept and retained for a period of three years. In the event of an appeal, the subject access request is retained for 6 years post closure of appeal.

Statistics
Statistics to ascertain how many individual right's requests has been received and whether they have been processed in accordance with the GDPR should be maintained and internally reported to provide assurance of compliance.

Right to Rectification (Article 16 and 19)
Overview
Individuals have the right to have inaccurate or incomplete personal data rectified under Article 16 of the GDPR. If a request for rectification is received we should take reasonable steps to check that the data is accurate and rectify the data if necessary; taking into account the arguments and evidence provided by the individual.

Processing the Request
The request should be logged and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply. Please see above.

In terms of taking reasonable steps; what steps are reasonable will depend on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort we should put into checking its accuracy and, if necessary, taking steps to rectify it. We may also take into account any steps we have already taken to verify the accuracy of the data prior to the challenge by the data subject.

The GDPR does not give a definition of the term accuracy. However, the Data Protection Act 2018 (DPA 2018) states that personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

If mistakes are recorded, it may be prudent to maintain the mistake but update the record to show the accurate information. For example, if a diagnosis for a condition is recorded on a patient's record which later is proved not to be the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified

It may also be difficult to argue that 'opinions' are inaccurate and therefore able to be rectified, but should be recorded as opinions on the record.

Whilst the request is being considered, the data should be restricted (in accordance with Article 18 – see section 5.5 below) until the data is rectified.

If we are satisfied that the information is accurate/complete then we must tell the individual that we will not be amending their data and provide them with the detail contained in section 5.2. Please ensure a note is recorded on the individual's record indicating that the individual challenged the accuracy of the data and their reasons for doing so.

If we have disclosed the personal data to other organisations/individuals, we must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort (Article 19). If asked to, we must also inform the individual about these recipients.

Right to Erasure (Article 17 and 19)

Overview

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child

Therefore the right of erasure will not apply in all circumstances, and we must establish whether the above conditions apply before we can process such a request.

Processing the Request

The request should be logged and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2. apply. Please see above.

As described above, we must then determine whether the right of erasure applies to the particular request.

Exemptions

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;

- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional)

If we have disclosed the personal data to others, we must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort (Article 19). If asked to, we must also inform the individuals about these recipients.

Where personal data has been made public in an online environment (such as social networks) reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable we should take into account available technology and the cost of implementation.

If we refuse to comply with the request for erasure due to the fact that it is manifestly unfounded or excessive we must adhere to the conditions set out in section 5.2 above.

Right to Restrict Processing (Article 18 and 19)

Overview

Individuals have the right to request the restriction or suppression of their personal data in particular circumstances. The restriction cannot be put in place indefinitely but we will need to have the restriction in place for a certain period of time. This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Processing the Request

The request should be logged and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply. Please see above.

Individuals have the right to request that their personal data is restricted in the following circumstances:

- the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:

- if an individual has challenged the accuracy of their data and asked for us to rectify it (Article 16), they also have a right to request that we restrict processing while we consider their rectification request; or
- if an individual exercises their right to object under Article 21(1), they also have a right to request us to restrict processing while we consider their objection request

Therefore, as a matter of good practice we should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

In order to restrict processing, we should consider the following options:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website

Once the data is restricted, we must not process the restricted data in any way except to store it unless:

- We have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest

If we have disclosed the personal data in question to others, we must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort (Article 19). If asked to, we must also inform the individual about these recipients.

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and we are investigating this; or
- the individual has objected to us processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of your legitimate interests, and we are considering whether our legitimate grounds override those of the individual

Once we have made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, we may decide to lift the restriction. Once we have done this we must inform the individual before we lift the restriction.

As noted above, these two conditions are linked to the right to rectification (Article 16) and the right to object (Article 21). This means that if we are informing the individual that we are lifting the restriction (on the grounds that we are satisfied that the data is accurate, or that our legitimate grounds override theirs) we should also inform them of the reasons for our refusal to act upon their rights under Articles 16 or 21. We will also need to inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek a judicial remedy

If we refuse to comply with the request for restriction due to the fact that it is manifestly unfounded or excessive we must adhere to the conditions set out in section 5.2 above.

Right to Data Portability (Article 20)

Overview

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

Processing the Request

The request should be logged and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply. Please see above

The right to data portability only applies when:

- Our lawful basis for processing this information is consent or for the performance of a contract; and
- We are carrying out the processing by automated means (i.e. excluding paper files)

The right to data portability only applies to personal data and allows data to be transferred from us as the controller to another controller (if the above conditions apply).

The data must be provided in a structured, commonly used and machine readable format. We may need to seek advice and assurance from the IT team to determine how

the data can be transferred. Further details on how the data can be transferred can be found on the ICO's guidance webpages under 'Right to Data Portability'. We are responsible for ensuring the data is transmitted securely.

We can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Please refer to section 5.2 for details on what information must be provided to the individual if we are refusing to comply with their request.

Right to Object (Article 21)

Overview

An individual has the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority
- Direct marketing (including profiling)
- Processing for the purposes of scientific/historical research and statistics

Processing the Request

The request should be logged and acknowledged without undue delay and at least within 48 hours of receipt.

The same conditions regarding timescales, ID and fees as explained in sections 5.2 apply. Please see above

Performance of a legal task or organisation's legitimate interests

Individuals must have an objection on "grounds relating to his or her particular situation".

We must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims

We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Direct Marketing Purposes

We must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse.

We must deal with an objection to processing for direct marketing at any time and free of charge. We must inform individuals of their right to object "at the point of first communication" and in our privacy notice. This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Research Purposes

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

We can refuse to comply with a right to objection if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Please refer to section 5.2 for details on what information must be provided to the individual if we are refusing to comply with their request.

Right Not To Be Subject To Automated Decision Making (Article 22)

Overview

The GDPR applies to all automated decision making and profiling. This Article sets out additional rules to protect individuals if we are carrying out solely automated decision-making that has a legal or similarly significant effect on an individual. Automated individual decision making must be made without human involvement, e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Solely automated individual decision-making - including profiling - with legal or similarly significant effects is restricted, although this restriction can be lifted in certain circumstances. We can only carry out solely automated decision-making with legal or similarly significant effects if the decision is:

- necessary for entering into or performance of a contract between an organisation and the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent

If we're using special category personal data we can only carry out processing described in Article 22(1) if:

- we have the individual's explicit consent; or
- the processing is necessary for reasons of substantial public interest

Profiling (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Profiling can be part of an automated decision-making process. The GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. For something to be solely automated there must be no human involvement in the decision-making process.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.
A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention

We must inform individual if we are using this form of processing and if we are, we must:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention, express their point of view or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended
- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects. If our processing does not match this definition then we can continue to carry out profiling and automated decision-making but we must still comply with the GDPR principles. We must identify and record our lawful basis for the processing. We need to have processes in place so people can exercise their rights. Individuals have a right to object to profiling in certain circumstances. We must bring details of this right specifically to their attention

5. External References

External References
As identified in the Individual Rights Policy.

Freedom of Information
If requested, this document may be made available as part of the Practice's commitment to transparency and compliance with the Freedom of Information Act.