Integrated Management System		Date	15/03/21
Title	Subject Access Request Policy	Issue	3
Ref	IMSM.017	Approved	N. Catton

Subject Access Request Policy

The online version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

Introduction

Individuals have the right under the Data Protection Act 1998 (DPA) and General Data Protection Regulation 2016 (GDPR), subject to certain exemptions, to have access to their personal records that are held by CIS Security Ltd. This is known as a 'subject access request' (SAR).

Requests may be received from members of staff, clients or any other individual who CIS has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, audio recordings and CCTV images etc.

CIS Security Ltd has developed this policy to guide staff in dealing with SAR's) that may be received. The aim of this policy is to inform staff on, how to advise those requesting SAR's on how to make a subject access request, how to recognise a subject access request and know what action to take on receipt. This procedure sets out the processes to be followed to respond to a subject access request. This is based on the Information Commissioner's Office Subject Access Code of Practice: ICO Subject Access Code of Practice.

1.0 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the GDPR Group and the Data Protection Officer (DPO). It is derived from several national codes and policies which are considered as best practice.

2.0 SCOPE

This policy applies to those members of staff that are directly employed by CIS Security Ltd and for whom CIS Security Ltd has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience, the organisations policies are also applicable whilst undertaking duties for or on behalf of CIS Security Ltd. This procedure applies to all third parties and others authorised to undertake work on behalf of CIS Security Ltd. The purpose of this procedure is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests.

3.0 POLICY PURPOSE AND AIMS

3.1 What is a Subject Access Request?

A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information about them, which is held by CIS Security Ltd. The Data Protection Legislation entitles all individuals to make requests for their own personal data to enable individuals to verify the lawfulness of how their information is being processed. An individual is not entitled to information relating to other people (unless they are acting on behalf of that person).

The request does not have to be in any particular form other than in writing, nor does it have to include the words 'subject access' or make any reference to the Data Protection Legislation. A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore be treated as a SAR in the normal way. The applicant must be informed of how the application is being dealt, under which legislation free of charge, except where the request is manifestly unfounded or excessive (see 3.4.5[4]).

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- » told whether any personal data is being processed
- » given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- » given a copy of the personal data, *and*
- » given details of the source of the data (where this is available)

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have (e.g. legal proceedings). There are also other restrictions on disclosing information in response to a SAR, for example where this would involve disclosing information about another individual. (e.g. CCTV footage that clearly shows other's identity).

3.2 How to recognise and action a Subject Access Request

For CIS Security Ltd to action a subject access request the following must be received:

- » The request must be made in writing; this may be by letter, fax, email or twitter. It is important to note that responses to SAR requests must be returned by a secure methodology, i.e. social

media must NOT be used to return information requested. However, where the applicant is not able to make the request in writing it can be received verbally and a record of the request made on the applicant's file.

- » Any fee levied - fees can only be levied where the request is deemed manifestly unfounded or excessive.
- » Proof of identity of the applicant and/or the applicant representative, and proof of right of access to another person's personal information, by reasonable means (See Appendix One).
- » Sufficient information to be able to locate the record or information requested.
- » All requests must be responded to without delay and at the latest within one month of receipt of the request. This time can be extended by a further two months where requests are complex or numerous. However, if this is the case you must inform the individual within one month of the receipt of the request and explain why the extension is necessary. General Data Protection Regulation 2016.

If the request relates to or includes information that should not be requested by means of a SAR (e.g. it includes a request for non-personal information) then, the request must be treated accordingly, e.g. as a FOI request where purely non-personal data is being sought or as two requests: one for the requester's personal data made under the DPA and GDPR; and another for the remaining, non-personal information made under FOIA.

Any requests made for non-personal information must be forwarded to the FOI Team at DPO@cis-security.co.uk. It is important to consider the requested information under the right legislation. This is because the test for disclosure under FOIA is to the world at large – not just the requester. If personal data is mistakenly disclosed under FOIA to the world at large, this could lead to a breach of the data protection principles.

All SAR requests received must be forwarded to the relevant head of department, e.g. staff requesting access to personnel records must be sent to Head of HR, without delay for it to be processed within the legal timescale. Where CIS Security Ltd processes a large quantity of information about an individual the GDPR permits you to ask the individual to specify the information the request relates to. The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- » Charge a reasonable fee considering the administrative costs of providing the information, *or*

» Refuse to respond.

Where you refuse to respond you must explain to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

3.3 Assisting and Advising Service Users on how to make a request

Where an individual is verbally making a request, you should advise that the will need to:

» Put the request in writing, detailing the information they are requesting and from which service to enable it to be located.

» Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request.

» A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So, it is important to ensure that you and your colleagues can recognise a SAR and deal with it in accordance with this procedure and forward immediately to the relevant service head.

» Advise the applicant to send the request to the appropriate head of service and provide contact details.

» To comply with equality legislation, where an applicant is unable to put the request in writing assistance should be given to them to make the request verbally, best practice would be to document the request details in an accessible format for the applicant and request them to confirm the details are correct. Applicants can be referred to the HR Team to obtain appropriate assistance in making their application.

» Note that responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed e.g. braille.

3.4 Requests made about or on behalf of other individual

3.4.1 General Third Party

A third party, e.g. solicitor, may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individual's consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney must be provided by the third party.

If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

3.4.2 Requests on Behalf of Children (unlikely to be applied to CIS)

Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them. Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. The Information Commissioner has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

The guardian or their nominated representative should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that, just because a child has capacity to make a SAR, that they also have capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so.

What matters is that the child can understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following should be taken into account:

- Where possible, 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.

3.4.3 Requests in respect of Crime and Taxation e.g. from the Police or HMRC

Requests for personal information may be made by the above authorities for the following purposes:

» The prevention or detection of crime

» The capture or prosecution of offenders, *and*

» The assessment or collection of tax or duty

A formal documented request signed by a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation. These types of requests must be considered by a senior manager and the decision on whether to share the information or not documented before any action is taken. Advice can be sought from the GDPR Group and DPO.

3.4.4 Court Orders

Any Court Order requiring the supply of personal information about an individual must be complied with.

3.4.5 Responding to Requests

It is essential that a log of all requests received is maintained, detailing: Appendix 4

» Date received

» Date response due (within one calendar month unless complex)

» Applicant's details

» Information requested

» Exemptions applied in respect of information not to be disclosed

» Details of decisions to disclose information without the data subject's consent

» Details of information to be disclosed and the format in which they were supplied

» When and how supplied, e.g. paper copy and postal method used to send them. Determine whether the person's request is to be treated as a routine enquiry or as a subject access request. If you would usually deal with the request in the normal course of business e.g. confirming

meeting/interview times or details of public meetings planned, then do so. The following are likely to be treated as formal subject access requests.

» "Please send me a copy of my HR file or concerns with my image on any CIS controlled CCTV". This can go to either the System Owner or through CIS.

» "I am a solicitor acting on behalf of my client and request a copy of his/her employment records, and appropriate authority is enclosed".

» The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.

1. Ensure adequate proof of the identity of both the data subject and the applicant, where this is a third party is obtained before releasing information requested, this may be in the form of documentation as detailed in Appendix One.
2. Ensure adequate information has been received to facilitate locating the information requested, locate the required information from all sources and collate it ready for review by an appropriate senior manager. This review is to ensure that the information is appropriate for disclosure, i.e. to ascertain whether any exemptions apply e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed or is information to be withheld due to ongoing formal investigations. Advice may be sought from the GDPR Group and DPO. Exemptions are detailed at Appendix Two.
3. Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual.
4. Generally CIS Security Ltd must provide a copy of the information free of charge. However, a 'reasonable fee' may be levied when a request is manifestly unfounded or excess, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.
5. Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact as soon as possible.
6. It must be determined whether the information is likely to change between receiving the request and sending the response. Routine ongoing business additions and amendments may be made to the personal information after a request is received, however the information must not be

altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under the Data Protection Act 1998.

7. Check whether the information collated contains any information about any other individuals and if so, consider:

» Is it possible to comply with the request without revealing information that relates to the third party?

Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party.

Where it is not possible to remove third party identifiers you must consider the following:

» Has the third party consented to the disclosure?

» Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party?

The following must be considered when trying to determine what reasonable circumstances are:

» Duty of confidence owed to the third party

» Steps taken to try and obtain consent

» Whether the third party can give consent, and any express refusals of consent from the third party. A record of the decision as to what third party information is to be disclosed and why it should be made. Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:

- Crime prevention and detection, including taxation purposes
- Negotiations with the requestor
- Management Forecasts
- Confidential References given by you
- Information used in research, historical or statistical purposes, *and*
- Information covered by legal professional privilege

Other exemptions are detailed at **Appendix Two**.

If the information requested, is held by the organisation and exemptions apply then a decision must be made as to whether you inform that applicant that the information is held but is exempt from disclosure

or whether you reply stating that no relevant information is held. A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing ongoing or potential investigations or undue harm or distress is to be avoided.

NB. It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered. If the information contains complex terms or codes, you must ensure that these terms and codes are explained in such a way that the information can be understood in lay terms.

Preparing the response:

- When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case, by the due date.
- A copy of the information should be supplied in a format agreed with the applicant for example if the request is received electronically, then the response should be returned in an electronic format. You have one calendar month to comply with the request starting from the date you receive all the information necessary to deal with the request and any fee that is required. It is an offence under the Data Protection Legislation and individuals can complain to the Information Commissioners Office or apply to a court if you do not respond within this time limit.

NB Under no circumstances should original records be sent to the applicant.

Remote access to records: Where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. (consider the access and available information through the Timegate portal).

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

Ensure that the information to be supplied is reviewed by an appropriate senior manager and written authorisation and / or agreement of exemptions applied is obtained for disclosure or non-disclosure of the information.

4.0 IMPLEMENTATION

This policy will be published on the CIS Security Ltd website and all staff will be made aware of its publication through communications and team meetings. Breaches of this policy may be investigated

and may result in the matter being treated as a disciplinary offence under CIS Security Ltd's disciplinary procedure.

5.0 TRAINING AND AWARENESS

The Senior Management Team and line managers are responsible for ensuring that all staff are aware of the policy which will be available via the CIS Security Ltd Intranet/website/internal communications. This policy is available on the company website and employee portal.

6.0 MONITORING AND AUDIT

Performance against the Information Governance Toolkit will be reviewed on an annual basis and used to inform the development of future procedural documents. This standard will be reviewed on a regular basis, and in accordance with the following on an as-and-when-required basis:

- legislative changes
- good practice guidance
- case law
- significant incidents reported
- new vulnerabilities, *and*
- changes to organisational infrastructure

7.0 POLICY REVIEW

The policy and procedure will be reviewed at least every year by the CIS Security Ltd SHEQ Manager and DPO in conjunction with relevant management review processes, with any changes made as required and the outcome published. Where review is necessary due to legislative change, this will happen immediately.

8.0 Appendices

APPENDIX ONE - REGISTRATION & AUTHENTICATION EXAMPLES OF DOCUMENTARY EVIDENCE

Please supply one from each of the following categories (copies only).

8.1 Personal identity

- Current signed passport
- Residence permit issued by Home Office to EU Nationals on sight of own country passport
- Current UK photocard driving licence
- Current full UK driving licence (old version) – old style provisional driving licences are not acceptable
- Current benefit book or card or original notification letter from the Department for Work and Pensions confirming the right to benefit
- Building industry sub-contractor's certificate issued by the Inland Revenue
- Recent Inland Revenue tax notification
- Current firearms certificate
- Birth certificate
- Adoption certificate
- Marriage certificate
- Divorce or annulment papers
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
- GV3 form issued to people who want to travel in the UK but do not have a valid travel document
- Home Office letter
- Police registration document
- HM Forces Identity Card

APPENDIX TWO – SUBJECT ACCESS REQUESTS EXEMPTIONS

Category	Exemption
National Security	Personal information that is held in respect of the maintenance of national security is exempt from disclosure.
Crime and Taxation	Section of the personal information contained in the records, or individual records that relate to the prevention and detection of crime or the apprehension or prosecution of offenders.
Health, Education and Social Work	Health exemptions are mentioned in Section 7 Social Work records exemptions comes under the Data Protection (Subject Access Modification) (Social Work) Order 2000 relates to personal information used for social work purposes: Where release of information may prejudice the carrying out of social work by causing serious harm to the physical or mental condition of the data subject or others. Certain third party's information can be released if they are a "relevant person" (a list is contained in the order) if release of the information does not cause serious harm to the relevant person's physical or mental condition, or with the consent of the third party.
Regulatory Activity	Personal data processed for the purposes of discharging it functions are exempt if the release of such information would prejudice the proper discharge of those functions.
Research, History Statistics	Where the personal data is used solely for research purposes and as long as resulting statistics are not made available which identify the person.
Legal Professional Privilege	Any correspondence to or from or documentation prepared for or by CIS's internal or external legal advisors may be exempt from disclosure and advice should always be sought relating this class of information.

Document Owner and Approval

The Managing Director is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the GDPR.

A current version of this document is available to all members of staff on the company website and Y:\ drive. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Board of Directors on 18/05/2018 and is issued on a version-controlled basis under the signature of the CIS Managing Director.

Signature:

Date: 18th May 2018
Date Reviewed 15/03/21

Change History Record

Ref	Issue	Description of Change	Approval	Date of Issue
IMSM.017	1	Initial issue	Managing Director	18.05.18
IMSM.017	2	Review of document	Managing Director	23.03.20
IMSM.017	3	Review of document	Managing Director	15.03.21