GDPR Policies

Contents

Louise Bradshaw the HR Manager is CAS's data officer in respect of its data protection activities and policies.

Data Protection Policy (GDPR compliant)

1. Introduction

1.1. This policy applies to the processing of personal data in manual and electronic records kept by Community Action Suffolk (CAS) in connection with its human resources function as described below. It also covers CAS's response to any data breach and other rights under the General Data Protection Regulation (GDPR).

2. Scope

2.1. This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

3. Meanings

3.1. "Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

3.2. "Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

3.3. "Criminal offence data" is data which relates to an individual's criminal convictions and offences.

3.4. "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.5. CAS makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of CAS, CAS will ensure that the third party takes such measures in order to maintain CAS's commitment to protecting data. In line with GDPR, CAS understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

4. Types of data held

4.1. Personal data is kept in personnel files or within CAS's HR and finance systems. The following types of data may be held by CAS, as appropriate, on relevant individuals:

- 4.1.1. Name, address, phone numbers - for individual and next of kin
- 4.1.2. CVs, application forms and other information gathered during recruitment
- 4.1.3. References from former employers
- 4.1.4. National Insurance numbers
- 4.1.5. Job title, job descriptions and pay grades
- 4.1.6. Conduct issues such as letters of concern, disciplinary proceedings
- 4.1.7. Holiday records
- 4.1.8. Internal performance information
- 4.1.9. Medical or health information
- 4.1.10. Sickness absence records
- 4.1.11. Tax codes
- 4.1.12. Terms and conditions of employment
- 4.1.13. Training details

4.2. Relevant individuals should refer to CAS's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

5. Data protection principles

5.1. All personal data obtained and held by CAS will:

- 5.1.1. Be processed fairly, lawfully and in a transparent manner
- 5.1.2. Be collected for specific, explicit, and legitimate purposes
- 5.1.3. Be adequate, relevant and limited to what is necessary for the purposes of processing
- 5.1.4. Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- 5.1.5. Not be kept for longer than is necessary for its given purpose
- 5.1.6. Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- 5.1.7. Comply with the relevant GDPR procedures for international transferring of personal data

5.2. In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- 5.2.1. The right to be informed
- 5.2.2. The right of access
- 5.2.3. The right for any inaccuracies to be corrected (rectification)
- 5.2.4. The right to have information deleted (erasure)
- 5.2.5. The right to restrict the processing of the data
- 5.2.6. The right to portability
- 5.2.7. The right to object to the inclusion of any information
- 5.2.8. The right to regulate any automated decision-making and profiling of personal data

6. Procedures

6.1. CAS has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

6.1.1. It appoints or employs employees with specific responsibilities for:

6.1.1.1. The processing and controlling of data

6.1.1.2. The comprehensive reviewing and auditing of its data protection systems and procedures

6.1.1.3. Overviewing the effectiveness and integrity of all the data that must be protected.

6.2. There are clear lines of responsibility and accountability for these roles.

6.3. It provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way

6.4. It provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially

6.5. It can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with

6.6. It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by CAS

6.7. It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. CAS understands that consent must be freely given, specific, informed and unambiguous. CAS will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time

6.8. It has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences

6.9. It is aware of the implications international transfer of personal data internationally

7. Access to data

7.1. Relevant individuals have a right to be informed whether CAS processes personal data relating to them and to access the data that CAS holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

7.1.1. A form on which to make a subject access request is available on the shared resources drive. The request should be made to the HR Manager.

7.1.2. CAS will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request

7.1.3. CAS will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous

7.2. Relevant individuals must inform CAS immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. CAS will take immediate steps to rectify the information.

7.3. For further information on making a subject access request, employees should refer to our subject access request policy.

8. Data disclosures

8.1. CAS may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

8.1.1. Any employee benefits operated by third parties

8.1.2. Disabled individuals - whether any reasonable adjustments are required to assist them at work

8.1.3. Individuals' health data - to comply with health and safety or occupational health obligations towards the employee

8.1.4. For Statutory Sick Pay purposes

8.1.5. HR management and administration - to consider how an individual's health affects his or her ability to do their job

8.1.6. The smooth operation of any employee insurance policies or pension plans

8.2. These kinds of disclosures will only be made when strictly necessary for the purpose.

9. Data security

9.1. CAS adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the data transfer security policy.

9.2. In addition, employees must:

9.2.1. Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them

9.2.2. Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people

9.2.3. Check regularly on the accuracy of data being entered into computers

9.2.4. Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them

9.2.5. Use computer screen blanking to ensure that personal data is not left on screen when not in use

9.3. Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless absolutely necessary and authorised by the Data Officer or Executive Team member. Where personal data is recorded on any such device it should be protected by:

9.3.1. Ensuring that data is recorded on such devices only where absolutely necessary

9.3.2. Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted

9.3.3. Ensuring that laptops or USB drives are not left lying around where they can be stolen

9.3.4. Failure to follow CAS's rules on data security may be dealt with via CAS's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

10. International data transfers

10.1. CAS does not transfer personal data to any recipients outside of the EEA.

11. Breach notification

11.1. Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of CAS becoming aware of it and may be reported in more than one instalment.

11.2. Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

11.3. If the breach is sufficient to warrant notification to the public, CAS will do so without undue delay.

12. Training

12.1. New employees must read and understand the policies on data protection as part of their induction.

12.2. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

12.3. The nominated data officer for CAS is trained appropriately in their role under the GDPR.

12.4. All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and CAS of any potential lapses and breaches of CAS's policies and procedures.

13. Records

13.1. CAS keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

14. Data protection compliance

14.1. The HR Manager is CAS's data officer in respect of its data protection activities.

Data Breach Notification Policy (GDPR compliant)

1. Introduction

1.1. CAS is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure it is kept securely. We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse.

1.2. The GDPR incorporates a requirement for certain types of personal data breaches to be notified to the supervisory authority and in some cases to the affected individuals. This policy sets out CAS's stance on taking action in line with GDPR if a breach were to occur.

2. Personal data breach

2.1. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

2.2. As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

- 2.2.1. Access by an unauthorised third party
- 2.2.2. Deliberate or accidental action (or inaction) by a data controller or data processer
- 2.2.3. Sending personal data to an incorrect recipient
- 2.2.4. Computing devices containing personal data being lost or stolen
- 2.2.5. Alteration of personal data without permission
- 2.2.6. Loss of availability of personal data

3. Notifiable breaches

3.1. For the purposes of this policy, a data breach will be notifiable when it is deemed by CAS as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on CAS's breach register.

3.2. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

3.3. When assessing the likelihood of the risk to people's rights and freedoms, CAS will consider:

- 3.3.1. The type of breach
- 3.3.2. The type of data involved including what it reveals about individuals
- 3.3.3. How much data is involved
- 3.3.4. The individuals involved e.g. how many are involved, how easy it is to identify them, whether they are children etc.

3.3.5. How bad the consequences for the individuals would be and
3.3.6. The nature of CAS's work and the resultant severity of a breach

4. Actions upon identification of breach

4.1. When CAS is made aware of a breach, it will undertake an immediate investigation into what happened and what actions must be taken to restrict any consequences. A determination will be made at that point whether the breach is deemed a notifiable breach and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

5. Timescales for notification to supervisory authority

5.1. Where a notifiable breach has occurred, CAS will notify the ICO without undue delay and at the latest within 72 hours of it becoming aware of the breach. If notification is made beyond this timeline, CAS will provide the ICO with reasons for this.

5.2. If it has not been possible to conduct a full investigation into the breach in order to give full details to the ICO within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the ICO to submit the remaining information.

6. Content of breach notification to the ICO

6.1. The following information will be provided when a breach is notified:

6.2. A description of the nature of the personal data breach including, where possible:
6.2.1. The categories and approximate number of individuals concerned and
6.2.2. The categories and approximate number of personal data records concerned
6.3. The name and contact details of the HR Manager where more information can be obtained
6.4. A description of the likely consequences of the personal data breach
6.5. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

7. Timescales for notification to affected individuals

7.1. Where a notifiable breach has occurred which is deemed to have a high risk to the rights and freedoms of individuals, CAS will notify the affected individuals themselves ie the individuals whose data is involved in the breach, in addition to the ICO. This notification will be made without undue delay and may, dependent on the circumstances, be made before the ICO is notified.

7.2. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

8. Content of breach notification to the affected individuals

8.1. The following information will be provided when a breach is notified to the affected individuals:

8.1.1. A description of the nature of the breach

8.1.2. The name and contact details of CAS's appointed data officer where more information can be obtained

8.1.3. A description of the likely consequences of the personal data breach

8.1.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

9. Record of breaches

9.1. CAS records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

Data Transfer Security Policy (GDPR compliant)

1. Introduction

1.1. CAS stores a large volume of information electronically. This policy governs the procedures to protect this information and sets out how data should be transferred in, and outside CAS, in a secure and protected way.

2. The law

2.1. Data storage is regulated by the General Data Protection Regulation. Standards are set out in the Regulation and the current Data Protection Act and one of the key points for consideration in a data transfer situation is that personal data must not be transferred to a country/territory outside the European Economic Area (EEA) unless that country/territory ensures appropriate safeguards.

3. Sensitive data

3.1. Sensitive data, for the purpose of this policy, it includes data which contains:

3.1.1. Personal details about an individual (including those which are classed as special categories of data including data relating to health and race etc)

3.1.2. Confidential data about CAS

3.1.3. Confidential data about goods, products or services

3.1.4. Confidential data about Company customers and suppliers

3.2. If employees have any doubt as to whether data is or is not 'sensitive data', employees must refer the matter to their the Data Officer or SMT lead.

4. Data transfers

4.1. Employees must seek consent from their the Data Officer or Executive Team member to authorise the transfer of sensitive data.

4.2. Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of CAS. Accordingly, before any data transfers are requested, the necessity of the transfer should be considered in advance.

4.3. After authorisation has been granted, the data must be referred to CAS IT Department so that it can be encrypted, compressed and password protected before it is sent.

5. Data transfers by post/courier

5.1. Data transfers which occur via physical media such as memory cards or CDs must only be dispatched via secure post. The use of first or second class Royal Mail is not permitted; only Special Delivery or Recorded Delivery should be used. For non-Royal Mail services, a secure courier service must be used with a signature obtained upon delivery.

5.2. The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

5.3. The recipient should be advised in advance that the data is being sent so that they are aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

6. Lost or missing data

6.1. If an employee discovers that data has been lost or is missing, the employee is required to inform their the Executive Team member immediately who will refer the matter to CAS's Data Officer.

6.2. CAS's Breach Notification Policy will be followed. An investigation will be initiated immediately to establish the events leading to the data loss/theft and to determine whether a breach of personal data has occurred. If it has, a determination will be made as to whether the breach is notifiable under that policy.

6.3. The Executive Team and Data Officer must consider referring a matter to the police if it is found that unauthorised individuals have accessed sensitive data. Data which is held in the correct encrypted, compressed and/or password protected formats, which has been accessed by an unauthorised individual, has been accessed unlawfully.

7. Negligent data transfers

7.1. Employees who fail to comply with the requirements of this policy are likely to have their actions considered as gross misconduct, which may result in summary dismissal. Personal data breaches may result in exceptionally large fines for CAS.

7.2. Employees must not be negligent when transferring sensitive data. Examples of negligence include failing to obtain authorisation from a the Data Officer or Executive Team member, failing to ensure CAS IT Department encrypted, compressed and password-protected data, or using non-secure post services which are not tracked or insured.

Data Subject Rights Policy (GDPR compliant)

1. Introduction

1.1. CAS processes many types of data concerning job applicants, employees, former employees, workers and contractors for various reasons. CAS is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure that the rights of data subjects, as set out in GDPR, are observed correctly.

2. Scope

2.1. This policy sets out the rights of the individuals as data subjects and the processes which should be followed in the event that the data subject wishes to exercise any such right.

3. Data subject rights

3.1. Under GDPR, you have the following rights in relation to your data:

3.1.1. The right to be informed
3.1.2. The right of access
3.1.3. The right for any inaccuracies to be corrected
3.1.4. The right to have information deleted
3.1.5. The right to restrict the processing of the data
3.1.6. The right to portability
3.1.7. The right to object to the inclusion of any information
3.1.8. The right to regulate any automated decision-making and profiling of personal data

4. The right to be informed

4.1. You have the right to be told how CAS processes your data and the reasons for the processing. In order to provide this information to you, CAS has a privacy notice to explain what data we collect about you, how we collect and process it, what we process it for and the lawful basis which permits us to process it. You can obtain a copy of the privacy notice from the HR Manager.

4.2. CAS also has a separate privacy notice applicable to job applicants, available from the HR Manager.

4.3. If CAS intends to use data already collected from you for a different reason than that already communicated, you will be informed of the new reason in advance.

5. The right of access

5.1. You have the right to access your personal data which is held by CAS. More information on this is available in CAS's Subject Access Request policy.

6. **The right for data to be corrected**

6.1. One of the fundamental principles underpinning data protection is that the data CAS processes about you will be accurate and up to date. You have the right to have your data corrected if it is inaccurate or incomplete.

6.2. If you wish to have your data rectified, you should do so by completing the Data Rectification Form which is available on the shared drive.

6.3. CAS will respond to a data rectification request within one month. Where the data rectification request is complex, CAS may extend the timescale for response from one month to three months. If this is the case, CAS will write to you within one month of receipt of the request explaining the reason for the extension.

6.4. If the response to your request is that CAS will take no action, you will be informed of the reasons for this and of your right to complain to the Information Commissioner and to a judicial remedy.

6.5. Where any data which has been rectified was disclosed to third parties in its unrectified form, CAS will inform the third party of the rectification where possible. CAS will also inform you of the third parties to whom the data was disclosed.

7. The right to have information deleted

7.1. You have the right to have your data deleted and removed from our systems where there is no compelling business reason for CAS to continue to process it.

7.2. You have a right to have your data deleted in the following circumstances:

7.2.1. Where the personal data is no longer necessary in relation to the purpose for which CAS originally collected or processed it

7.2.2. Where you have withdrawn your consent to the continued processing of the data and there is no other lawful basis for CAS to continue processing the data

7.2.3. Where you object to the processing and CAS has no overriding legitimate interest to continue the processing

7.2.4. The personal data has been unlawfully processed

7.2.5. The personal data has to be deleted due to a legal obligation

7.3. If you wish to make a request for data deletion, you should complete the Data Deletion Request form which is available on the shared drive.

7.4. Upon receipt of a request, CAS will delete the data unless it is processed for one of the following reasons:

7.4.1. To exercise the rights of freedom of expression and information

7.4.2. For CAS to comply with a legal requirement

7.4.3. The performance of a task carried out in the public interest or exercise of official authority

7.4.4. For public health purposes in the public interest

7.4.5. Archiving purposes in the public interest, scientific historical research or statistical purposes

7.4.6. The defence of legal claims

7.5. Where your request is not complied with because of the one of the above reasons, you will be informed of the reason. Where your request is to be complied with, you will be informed when the data has been deleted.

7.6. Where the data which is to be deleted has been shared with third parties, CAS will inform those third parties where this is possible. However, where this notification will cause a disproportionate effect on CAS, this notification may not be carried out.

8. The right to restrict the processing of data

8.1. You have the right to restrict the processing of your data in certain circumstances. Restricting CAS from processing your data means that CAS will continue to hold the data but will stop processing it.

8.2. CAS will be required to restrict the processing of your personal data in the following circumstances:

8.2.1. Where you tell CAS that the data it holds on you is not accurate. Where this is the case, CAS will stop processing the data until it has taken steps to ensure that the data is accurate

8.2.2. Where the data is processed for the performance of a public interest task or because of CAS's legitimate interests and you have objected to the processing of data. In these circumstances, the processing may be restricted whilst CAS considers whether its legitimate interests mean it is appropriate to continue to process it

8.2.3. When the data has been processed unlawfully

8.2.4. Where CAS no longer needs to process the data but you need the data in relation to a legal claim

8.3. If you wish to make a request for data restriction, you should complete the Data Restriction Request form which is available on the shared drive.

8.4. Where data processing is restricted, CAS will continue to hold the data but will not process it unless:

8.4.1. You consent to the processing

8.4.2. Processing is required in relation to a legal claim

8.5. Where the data to be restricted has been shared with third parties, CAS will inform those third parties where this is possible. However, where this notification will cause a disproportionate effect on CAS, this notification may not be carried out.

8.6. Where CAS is to lift any restriction on processing, you will be informed in advance.

9. The right to data portability

9.1. You have the right to obtain the data that CAS processes on you and use it for your own purposes. This means you have the right to receive the personal data that you have provided to CAS in a structured machine readable format and to transmit the data to a different data controller.

9.2. This right applies in the following circumstances:

9.2.1. Where you have provided the data to CAS

9.2.2. Where the processing is carried out because you have given CAS your consent to do so

9.2.3. Where the processing is carried out in order to perform the employment contract between you and CAS

9.2.4. Where processing is carried out by automated means

9.3. If you wish to exercise this right, please speak to the HR Manager.

9.4. Where a request for data portability is received, CAS will respond without undue delay, and within one month at the latest. Where the request is complex or CAS receives a number of requests, CAS may extend the timescale for response from one month to three months. If this is the case, CAS will write to you within one month of receipt of the request explaining the reason for the extension.

9.5. Where CAS is to comply with your request, you will receive the data in a structured and machine readable form. You will not be charged for the provision of this data. Upon request, CAS will transmit the data directly to another organisation if our IT systems are compatible with those of the recipient.

9.6. If the response to your request is that CAS will take no action, you will be informed of the reasons for this and of your right to complain to the Information Commissioner and to a judicial remedy.

9.7. The right to portability is different from the right to access. Although both involve a right to access your personal data, the personal data to be accessed is not the same. The right to access your data under the right to portability includes only personal data as described above. Access to data under the right of access includes all personal data relating to you, including that which has not been provided to CAS by you.

10. The right to object to the inclusion of data

10.1. You have a right to object to the processing of your data in certain circumstances. This means that you have the right to require CAS to stop processing your data. In relation to your employment with CAS, you may object to processing where it is carried out:

10.1.1. In relation to CAS's legitimate interests
10.1.2. For the performance of a task in the public interest
10.1.3. In the exercise of official authority or
10.1.4. For profiling purposes

10.2. If you wish to object, you should do so by completing the Data Processing Objection form which is available on the shared drive.

10.3. Where you object to processing, CAS will stop the processing activity objected to unless:

10.3.1. CAS can demonstrate compelling legitimate reasons for the processing which are believed to be more important than your rights
10.3.2. The processing is required in relation to legal claims made by, or against, CAS

10.3.3. If the response to your request is that CAS will take no action, you will be informed of the reasons.

11. Rights in relation to automated decision making

11.1. You have the right not to have decisions made about you solely on the basis of automated decision making processes where there is no human intervention, where such decisions will have a significant effect on you. However, CAS does not make any decisions based on such processes.

Subject Access Request Policy (GDPR compliant)

1. Introduction

1.1. Under the General Data Protection Regulation (GDPR), you have a right to receive confirmation that an organisation processes your personal data, and also a right to access that data so that you may be aware of it and are able to verify the lawfulness of the processing. The process for doing so is called a subject access request and this policy sets out the procedure to be undertaken when such a request is made by you regarding data processed about you by CAS.

2. What is personal data?

2.1. "Personal data" is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

2.2. "Special categories of personal data" includes information relating to:

- 2.2.1. Race
- 2.2.2. Ethnic origin
- 2.2.3. Politics
- 2.2.4. Religion
- 2.2.5. Trade union membership
- 2.2.6. Genetics
- 2.2.7. Biometrics (where used for ID purposes)
- 2.2.8. Health
- 2.2.9. Sex life
- 2.2.10. Sexual orientation

3. Information you are entitled to

3.1. When you make a subject access request, you will be informed of:

- 3.1.1. Whether or not your data is processed and the reasons for the processing of your data
- 3.1.2. The categories of personal data concerning you
- 3.1.3. Where your data has been collected from if it was not collected from you
- 3.1.4. Anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security
- 3.1.5. How long your data is kept for (or how that period is decided)
- 3.1.6. Your rights in relation to data rectification, erasure, restriction of and objection to processing
- 3.1.7. Your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed
- 3.1.8. The reasoning behind any automated decisions taken about you.

4. Making a subject access request

4.1. Subject access requests must be made in writing and can be made in either hard copy format or electronically. A copy of the form for making a request can be found on the shared drive however making a request in this format is not a requirement.

Including specific details of the data you wish to see in your request will enable a more efficient response from CAS. We may need to contact you for further details on your request if insufficient information is contained in the original request.

4.2. Requests may be made by you personally or by a third party e.g. a solicitor acting on your behalf. We will request evidence that the third party is entitled to act on your behalf if this is not provided at the same time as the request is made.

5. Upon receiving a subject access request

5.1. CAS will comply with your request without delay and at the latest within one month unless one of the following applies:

5.1.1. In some cases, we will be unable to supply certain pieces of information that you have requested. This may be because it is subject to legal privilege or relates to management planning. Where this is the case, CAS will inform you that your request cannot be complied with and an explanation of the reason will be provided

5.1.2. We require extra time because the requests are complex or numerous. In these circumstances, CAS will write to you within one month of receipt of your request to explain why an extension is required. Where an extension is required, information will be provided within three months of the request.

5.2. Before supplying the data (where appropriate) we may contact you asking for proof of identity. You must produce this evidence for your request to be complied with.

5.3. Your request will normally be complied with free of charge. However, we may charge a reasonable fee if the request is manifestly unfounded or excessive, or if it is repetitive. In addition, we may charge a reasonable fee if you request further copies of the same information. The fee charged will be based on the administrative cost of providing the information requested.

6. Refusing a request

6.1. CAS may refuse to comply with a subject access request if it is manifestly unfounded or excessive, or if it is repetitive. In these circumstances, we will write to you without undue delay and at the latest within one month of receipt to explain why we are unable to comply. You will be informed of the right to complain to the Information Commissioner and to a judicial remedy.

7. Enforced subject access requests

7.1. Forcing employees to obtain information via a subject access request, usually in relation to an individual's criminal record, is a criminal offence. No employee of CAS will be required to make a subject access request.

These policies are not contractual and may be amended at any time if it is considered appropriate to do so.

Issue & revision history

Date	Author	Version	Details
1.5.2020	Collis Consulting	1.0	LB Review – Changed role titles throughout and made minor amendments to wording
18.5.2020	Collis Consulting	1.0	ET Review – No amendments made
20.5.2020	Collis Consulting	1.1	Board review – Amendments made to add name of data officer on title page and reference procedures