SCCU EMPLOYEE DATA PROTECTION POLICY

SCCU LIMITED

VERSION 3.0

Contents

Version Control

VERSION	REVIEWER NAME	DATE	NEXT REVIEW	COMMENTS
3.0	Liam Morrissey	August 2021	01/08/2022	Update to previous.

Introduction

1. This policy applies to the processing of personal data in manual and electronic records kept by SCCU.
2. It also covers SCCU's response to any data breach and other rights under the General Data Protection Regulation.

Scope

3. This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors.
4. These groups are referred to in this policy as relevant individuals or employees.
5. Learners, potential learners and stakeholders are referred to as 'clients' throughout.

Definitions

6. "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.
7. "Special categories of personal data" is data that 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).
8. "Criminal offence data" is data that relates to an individual's criminal convictions and offences.
9. "Data processing" is any operation or set of operations that are performed on personal data or 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.

SCCU Data Protection Commitments

10. SCCU commits to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate), is processed in line with GDPR

2018/UK GDPR 2021 and domestic laws and all its employees conduct themselves in line with this, and other related policies.

11. Where third parties process data on behalf of SCCU, SCCU will ensure that the third party takes such measures to maintain SCCU's commitment to protecting data.
12. In line with GDPR, SCCU 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.

Types Of Data Held

13. Personal data is kept in personnel files and within SCCU's IT system.
14. The following types of data may be held by SCCU, as appropriate, on relevant individuals:
    - Name, address, phone numbers - for individual and next of kin.
    - CVs and other information gathered during recruitment.
    - References from former employers.
    - National Insurance numbers.
    - Job title, job descriptions and pay grades.
    - Conduct issues such as letters of concern, disciplinary proceedings.
    - Holiday records.
    - Internal performance information.
    - Medical or health information.
    - Sickness absence records.
    - Tax codes.
    - Terms and conditions of employment.
    - Training details.
15. We hold and process this data to meet our contractual and legal obligations and for legitimate business reasons.

Data Protection Principles

16. All personal data obtained and held by SCCU will:
    - Be processed fairly, lawfully and in a transparent manner.
    - Be collected for specific, explicit, and legitimate purposes.
    - Be adequate, relevant, and limited to what is necessary for processing.
    - Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
    - Not be kept for longer than is necessary for its given purpose.
    - 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 organisational measures.
    - Comply with the relevant GDPR procedures for international transferring of personal data.
17. Personal data will be processed in recognition of an individuals' data protection rights, as follows:
    - The right to be informed.
    - The right of access.
    - The right for any inaccuracies to be corrected (rectification).
    - The right to have information deleted (erasure).
    - The right to restrict the processing of the data.
    - The right to portability.
    - The right to object to the inclusion of any information.
    - The right to regulate any automated decision-making and profiling of personal data.

Data Protection Procedures

18. SCCU has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access.
19. We appoint people with specific responsibilities for:
    - The processing and controlling of data.
    - The comprehensive reviewing and auditing of its data protection systems and procedures.
    - Overviewing the effectiveness and integrity of all the data that must be protected.
20. We provide information to our employees on their data protection rights, how we use their personal data, and how we protect it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
21. We provide our 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 the information confidentially
22. We can account for all personal data we hold, where it comes from, who it is shared with and who it might be shared with.
23. We carry out risk assessments as part of our reviewing activities to identify any vulnerabilities in our 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 SCCU.
24. SCCU recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing, and retaining their personal data, and regularly reviews our procedures for doing so, including the audit trails that are needed and are followed for all consent decisions.
25. SCCU understands that consent must be freely given, specific, informed, and unambiguous.
26. SCCU 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.

27. SCCU has the appropriate mechanisms for detecting, reporting, and investigating suspected or actual personal data breaches, including security breaches. We are aware of our duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner and are aware of the possible consequences.
28. We are aware of the implications international transfer of personal data internationally.

Access to Data

29. Relevant individuals have a right to be informed whether SCCU processes personal data relating to them and to access the data that SCCU holds about them.
30. Requests for access to this data will be dealt with under the following summary guidelines:
    - Subject access request should be made to a Director.
    - SCCU 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.
    - SCCU 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.
31. Relevant individuals must inform SCCU immediately, if they believe that the data is inaccurate, either as a result of a subject access request or otherwise and SCCU will take immediate steps to rectify the information.

Data Disclosures

32. SCCU may be required to disclose certain data/information to any person.
33. The circumstances leading to such disclosures include:
    - Any employee benefits operated by third parties.
    - Disabled individuals - whether any reasonable adjustments are required to assist them at work, and they have consented to this information being shared.
    - Individuals' health data - to comply with health and safety or occupational health obligations towards the employee.

- For statutory sick pay purposes.
- HR management and administration - to consider how an individual's health affects his or her ability to do their job.
- The smooth operation of any employee insurance policies or pension plans.

34. For a legitimate legal reason for example if court ordered, or in the event of a safeguarding concern or criminal offence.
35. These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security

36. SCCU adopts procedures designed to maintain the security of data when it is stored and transported.
37. In addition, as an employee you must:
    - Ensure that all files or written information of a confidential nature, such as client information, are stored securely and are only accessed by people who have a need and a right to access them;
    - Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people;
    - Check regularly on the accuracy of data being entered into computers;
    - 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; and
    - Use computer screen blanking to ensure that personal data is not left on screen when not in use.
38. Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices unless authorised by a Director.
39. Where personal data is recorded on any such device it should be protected by:
    - Ensuring that data is recorded on such devices only where necessary;
    - 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; and

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

International Data Transfers

40. SCCU does not transfer personal data to any recipients outside of the EEA.

Breach Notification

41. 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 SCCU becoming aware of it and may be reported in more than one instalment.
42. Individuals will be informed directly if the breach is likely to result in a high risk to the rights and freedoms of that individual.
43. If the breach is sufficient to warrant notification to the public or those affected, SCCU will do so without undue delay.

Training

44. New employees must read and understand the policies on data protection as part of their induction.
45. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.
46. The nominated data controller/auditors/protection officers for SCCU have trained appropriately in their roles under the Data Protection Acta and GDPR articles.
47. 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 SCCU of any potential lapses and breaches of SCCU's policies and procedures.

Non-Compliance

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