GDPR AND 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. The European General Data Protection Regulation (GDPR) 2018 and the UK GDPR 2021 imposes a specific obligation on Data Controllers (owners) or Processors (data storage or users) concerning their vendor relationships.
2. The GDPR requires companies to conduct appropriate due diligence on data Processors and to have contracts containing specific provisions relating to data protection.
3. Each of the Agreements contains provisions requiring each party to comply with all applicable laws.
4. For this policy, SCCU may take the form of a Data Processor or Controller through its organisational structure.

Definitions

5. For purposes of this Agreement, "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any additional implementing legislation, rules or regulations that are issued by applicable supervisory authorities.
6. Words and phrases in this agreement shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:
    A. "**Personal Data**" has the meaning to give it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person," but only to the extent such Personal Data pertain residents of the European Economic Area (EEA) or are otherwise subject to the GDPR.
    B. "**Personal Data Breach**" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed."
    C. "**Processing**" has the meaning given to it in Article 4(2) of the GDPR: "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;"

D. "**SubProcessor**" means any Processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes Personal Data" on behalf of SCCU (including any affiliate of SCCU).

E. "**Transfer**" means to disclose or otherwise make Personal Data available to a third party (including any affiliate or SubProcessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

GDPR and Data Protection Policy

7. Following GDPR Article 28(1), SCCU, whether it takes the form of the Data Processor or Controller represents that it has implemented appropriate technical and organisational measures in such a manner that it's the processing of Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

8. Following GDPR Article 28(2), SCCU shall not engage any SubProcessor without prior specific or general written authorisation of The Licensor. In the case of general written authorisation, SCCU shall inform the Data Controller of any intended changes concerning the addition or replacement of other Sub Processors and allow The Data Controller to object to such changes.

9. SCCU shall also comply with the requirements for sub-processing as outlined in Article 28(4), namely that the data protection obligations set forth herein (and as may otherwise be agreed by SCCU in the Agreements) such be imposed upon the SubProcessor so that SCCU's contract with the SubProcessor contains sufficient guarantees that the processing will meet the requirements of the GDPR.

10. Following GDPR Article 28(3), the following terms are incorporated by reference into the Agreements:

    a) SCCU shall only process the Personal Data only (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from The Licensor, including with regard to any Transfers, and (iii) as needed to comply with the law (in which case, SCCU shall provide prior notice to the Data Controller of such legal requirement, unless that law prohibits this disclosure);

    b) SCCU shall ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) SCCU shall take all security measures required by GDPR Article 32, namely:

i. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, SCCU shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

ii. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

iii. SCCU shall take steps to ensure that any natural person acting under the authority of SCCU who has access to Personal Data does not process them except on instructions from the Data Controller unless he or she is required to do so by EEA Member State law.

11. Taking into account the nature of the processing, SCCU shall reasonably assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of The Licensor's obligation to respond to requests for exercising the data subject's rights;

12. Taking into account the nature of processing and the information available to SCCU, the Processor shall comply with (and shall reasonably assist the Data Controller to comply with) the obligations regarding Personal Data Breaches (as outlined in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as outlined in GDPR Article 36);

13. At The Licensor's discretion, SCCU shall delete or return all the Personal Data to the Data Controller after the end of the provision of services relating to Processing, and delete existing copies unless applicable EEA member state law requires the storage of the Personal Data;

14. SCCU shall provide the Data Controller with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to

audits, including inspections, conducted by the Data Controller or another auditor mandated by The Licensor; and

15. SCCU shall immediately inform other parties if, in its opinion, an instruction infringes the GDPR other Union or Member State data protection provisions.
16. SCCU will not transfer any Personal Data (and shall not permit its subProcessors to Transfer any Personal Data) without the prior consent of The Licensor.
17. SCCU understands that the controller must approve and document that adequate protection for the Personal Data will exist after the transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the transfer exists.
18. SCCU will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. The Processor will notify the Data Controller without undue delay in the event of any Personal Data Breach.
19. SCCU shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for the Data Controller) Processor shall make them available to the Data Controller upon request.

Data Protection Principles – Learners and Staff

20. SCCU will comply with the following data protection principles when processing personal information:

    - We will process personal information lawfully, fairly and in a transparent manner;
    - We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
    - We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes;
    - We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
    - We will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The Basis for Processing Personal Information – Learners and Staff

21. Concerning any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, for example:
    - That the data subject has consented to the processing;
    - That the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
    - That the processing is necessary for compliance with a legal obligation to which SCCU is subject;
    - That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
    - That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
        - That the processing is necessary for legitimate interests of SCCU or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

    o Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose);

    o Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.

    o Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).

    o Where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and

- Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

- Determine whether SCCU's legitimate interests are the most appropriate basis for lawful processing, we will:

  - Conduct a legitimate interest's assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

  - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

  - Keep the LIA under review, and repeat it if circumstances change; and

  - Include information about our legitimate interests in our relevant privacy notice(s).

Individual Rights – Leaners and Staff

22. People have the following rights concerning their personal information:

- To be informed about how, why and on what basis that information is processed.

- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the SAR Policy information.

- To have data corrected if it is inaccurate or incomplete;

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten);

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim; and

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering

whether the organisation's legitimate grounds override your interests).

- If you wish to exercise any of the rights in the paragraphs above, please contact the Data Protection Officer.