Axcelera Ltd (AXCELERA)

Data Retention Policy

CONTENTS

1. Introduction

This policy outlines the responsibilities of Axcelera Ltd (AXCELERA), a company registered in England under number 15353435, with its registered office at 124 City Road, London, United Kingdom, EC1V 2NX ("the Company"), regarding the retention of personal data collected, held, and processed by the Company in compliance with The Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation ("GDPR").

According to the GDPR, "personal data" refers to any information related to an identified or identifiable natural person (a "data subject"). An identifiable natural person is someone who can be identified, either directly or indirectly, particularly through an identifier like a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also covers "special category" personal data, also known as "sensitive" personal data. This category includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data must be kept in a format allowing the identification of data subjects for no longer than necessary for the purposes for which the personal data is processed. In specific cases, personal data may be retained for extended periods if processed for archiving purposes in the public interest, scientific or historical research, or statistical purposes, subject to the implementation of appropriate technical and organisational measures mandated by the GDPR to protect such data..

Additionally, the GDPR encompasses the right to erasure, commonly known as "the right to be forgotten." Data subjects possess the entitlement to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) When the personal data is no longer required for the purpose for which it was originally collected or processed (as mentioned above);

b) If the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data, and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e., in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

This policy delineates the categories of personal data retained by the Company for purposes including recruitment and resourcing, marketing, internal administration, and client delivery. It specifies the durations for which this personal data will be retained, the criteria governing the establishment and periodic review of these durations, and the procedures for deletion or disposal.

For comprehensive information on additional aspects of data protection and compliance with the GDPR, kindly refer to the Company's Data Protection Policy..

2. **Aims and Objectives**

2.1 The principal objective of this policy is to establish guidelines for the retention of personal data, with a focus on adhering to the limits outlined and acknowledging the data subject's rights to erasure. This policy is designed to facilitate the Company's full compliance with its obligations and the rights conferred upon data subjects by the GDPR.

2.2 Furthermore, beyond safeguarding the rights of data subjects, this policy seeks to enhance the efficiency of data management by preventing the retention of excessive amounts of data within the Company.

3. **Scope**

3.1 This Policy is applicable to all personal data held by the Company and to third-party data processors engaged in processing personal data on behalf of the Company..

3.2 The personal data maintained by the Company is stored through various means and in different locations:

a) On third-party servers operated by different suppliers, as specified in the Directory of Data, Assets, Risk, Systems & Retention Schedule, and situated in areas defined within the same directory;

b) On laptop computers and other mobile devices provided by the Company to its employees;

c) On computers and mobile devices owned by employees, agents, and sub-contractors, utilised in accordance with the Company's Data Security Policy;

d) In physical records stored in the AXCELERA CEO's office;

4. **Data Subject Rights and Data Integrity**

All personal data retained by the Company is managed in compliance with the GDPR and the rights afforded to data subjects outlined in the Company's Data Protection Policy.

4.1 Data subjects are provided comprehensive information about their rights, the specific personal data held by the Company, its utilisation, and the duration of its retention (or, if a fixed retention period cannot be established, the criteria guiding data retention decisions).

4.2 Data subjects retain control over their personal data held by the Company, including the right to rectify inaccurate data, request the deletion or disposal of their personal data (beyond the specified retention periods in this Data Retention Policy), restrict the Company's use of their personal data, exercise data portability rights, and avail themselves of additional rights related to automated decision-making and profiling, as detailed in Parts 14 to 20 of the Company's Data Protection Policy.

5. **Technical and Organisational Data Security Measures**

5.1 The Company has implemented the following technical measures to ensure the security of personal data. Further details can be found in Parts 22 to 26 of the Company's Data Protection Policy:

a) All emails containing personal data must be encrypted;

b) Personal data may only be transmitted over secure networks;

c) Personal data may not be transmitted over a wireless network if a reasonable wired alternative is available;

d) When sending personal data via facsimile transmission, the recipient must be informed in advance and be ready to receive it;

e) When transferring personal data in hardcopy form, it should be directly handed to the recipient;

f) All physically transferred personal data should be placed in a suitable container labelled as "confidential.";

g) Personal data may not be shared informally, and formal requests for access to any personal data should be directed to the Data Protection Team at data@axcelera.co.uk

h) Secure storage is required for all hardcopies of personal data and any electronic copies stored on physical media;

i) No personal data may be transferred to Users without proper authorisation, regardless of whether they are working on behalf of the Company;

j) Personal data should be handled with care, and it should not be left unattended or visible;

k) Computers used to view personal data must be locked before being left unattended;

l) Storage of personal data on mobile devices, whether owned by the Company or others, requires formal written approval from the CEO and compliance with instructions and limitations specified at the time of approval, for no longer than necessary;

m) Transfer of personal data to any device personally owned by a User is prohibited unless the User agrees to comply fully with the Company's Data Protection Policy and the GDPR;

n) Electronic storage of personal data should be regularly backed up in accordance with the Directory of Data, Assets, Risk, Systems & Retention Schedule, with backups stored in locations specified by the Directory and encrypted where possible;

o) Electronic copies of personal data should be securely stored using passwords and encryption;

p) Passwords used to protect personal data must be changed regularly and meet security standards;

q) Passwords must not be written down or shared; if forgotten, they must be reset using the appropriate method. IT staff do not have access to passwords;

r) All software should be kept up-to-date, with security-related updates installed promptly;

s) Installation of software on Company-owned computers or devices requires approval; and

t) In instances where the Company utilises personal data for marketing endeavours, it is incumbent upon the Marketing Manager to ensure the requisite consent is obtained. Additionally, the Marketing Manager is tasked with verifying that no data subjects have exercised their option to opt out, whether through direct communication or by means of a third-party service such as the TPS.

5.2 The Company has implemented a series of organisational measures to safeguard the security of personal data. For comprehensive details, please refer to Part 27 of the Company's Data Protection Policy. These measures include:

a) Ensuring that all Users are fully informed about both their individual responsibilities and the Company's obligations under the GDPR and its Data Protection Policy;

b) Granting access to personal data held by the Company only to Users who require it for the performance of their work;

c) Providing appropriate training to all Users responsible for handling personal data;

d) Implementing adequate supervision for Users dealing with personal data;

e) Encouraging Users handling personal data to exercise discretion and caution in all discussions related to such data;

f) Regularly evaluating and reviewing methods of collecting, holding, and processing personal data;

g) Conducting periodic evaluations and reviews of the performance of Users handling personal data;

h) Ensuring that all Users dealing with personal data are contractually bound to comply with the GDPR and the Company's Data Protection Policy;

i) Holding all Users handling personal data accountable for ensuring that others under their purview adhere to the conditions outlined in the GDPR and the Company's Data Protection Policy;

j) Imposing indemnification obligations on Users handling personal data in the event of their failure to fulfil obligations under the GDPR and/or the Company's Data Protection Policy. This indemnification covers any associated costs, liability, damages, loss, claims, or proceedings arising from such failures.

6. **Data Disposal**

Upon the conclusion of the designated data retention periods outlined in the Company's Directory of Data, Assets, Risk, Systems & Retention Schedule, or in the event a data subject exercises their right to request the erasure of their personal data, the handling of such data shall adhere to the following procedures:

6.1 Personal data stored electronically, including any associated backups, will be securely deleted in accordance with the prescribed method specified in the Directory of Data, Assets, Risk, Systems & Retention Schedule;

6.2 Special category personal data stored electronically, along with its backups, will be securely deleted utilising the method delineated in the Directory of Data, Assets, Risk, Systems & Retention Schedule;

6.3 Personal data maintained in hardcopy format will undergo secure shredding procedures as per the guidelines set forth in the Directory of Data, Assets, Risk, Systems & Retention Schedule, followed by appropriate recycling measures.

6.4 While the Company presently does not possess any Special category personal data stored in hardcopy form, the hypothetical scenario is addressed as follows: if such data were to exist, it would undergo secure shredding in accordance with the specifications outlined in the Directory of Data, Assets, Risk, Systems & Retention Schedule, followed by recycling protocols.

7. **Data Retention**

7.1 In adherence to legal obligations, the Company will not retain personal data beyond the necessary duration aligned with the purpose(s) for which the data is collected, held, and processed, as previously indicated.

7.2 Varied types of personal data utilised for distinct purposes will be subject to different retention periods, periodically reassessed, as outlined below.

7.3 When determining or revisiting retention periods, the following considerations shall be taken into account:

a) The Company's objectives and requirements;

b) The nature of the specific personal data;

c) The purpose(s) for collecting, holding, and processing the data in question;

d) The Company's legal basis for the collection, holding, and processing of that data;

e) The category or categories of data subjects associated with the data;

f) Company legislation basis, such as HMRC, Companies House, etc.

7.4 If it proves impractical to specify an exact retention period for a particular category of data, criteria will be formulated to govern the determination of the data's retention. This approach ensures that the data in question, along with its retention, undergoes periodic reviews in alignment with the established criteria.

7.5 Notwithstanding the predefined retention periods, certain personal data may be deleted or disposed of before the expiration of its designated retention period. This decision may be prompted by internal Company considerations, including requests from data subjects or other pertinent factors.

7.6 In specific instances, it might be necessary to retain personal data for extended periods for archiving purposes in the public interest, scientific or historical research, or statistical purposes. Such extended retention will be subject to the implementation of appropriate technical and organisational measures in accordance with the GDPR, ensuring the protection of the rights and freedoms of data subjects.

8. **Roles and Responsibilities**

8.1 The oversight of this Policy's implementation and the monitoring of compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and the GDPR, along with other applicable data protection legislation, falls under the purview of the Data Protection Team.

8.2 Within their designated functional areas of responsibility, the Data Protection Team assumes direct responsibility for ensuring compliance with the prescribed data retention periods outlined in the Directory of Data, Assets, Risk, Systems & Retention Schedule.

8.3 For any inquiries related to this Policy, the retention of personal data, or any other aspect of GDPR compliance, individuals are encouraged to direct their questions to the Data Protection Team.

9. Terms and Conditions

The Company

Axcelera Ltd (AXCELERA), a company registered in England under number 15353435, whose registered office is at 124 City Road, London, United Kingdom, EC1V 2NX

Data Controller

The entity that determines the purposes, conditions and means of the processing of personal data

Data Processor

The entity that processes data on behalf of the Data Controller

Data Protection Authority

National authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Team (DPT)

An team of experts on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject

A natural person whose personal data is processed by a controller or processor

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Hard data

Any data that is stored non-electronically, for example, but not exclusively, printed data on paper

Personal Data

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment

A tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing

Any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling

Any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation

A binding legislative act that must be applied in its entirety across the Union

Soft data

Any data that is stored electronically

Subject Access Right

Also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

The User

Principals, Regional Directors, consultants, agents, contractors, and/or employees, including part-time, temporary, or contract employees or other person working on behalf of the Company

10. Implementation of Policy

This Policy shall be deemed effective as of 23rd December 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

11. Related legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

12. Feedback and suggestion

Users may provide feedback and suggestions about this document by emailing data@axcelera.co.uk.