

Kadence Data Subjects Policy

1. INTRODUCTION

This policy outlines the rights of individuals (data subjects) regarding their personal data in compliance with the **General Data Protection Regulation (GDPR)** and **Data Protection Act 2018**. As a data controller, **Kadence** (now updated to reflect the organization's name or brand) ensures these rights are implemented appropriately and transparently, subject to legal exemptions.

2. PURPOSE AND OBJECTIVES

The purpose of this policy is to define Kadence's approach to upholding data subjects' rights, specify how requests are managed, and identify circumstances under which the organization may decline or be exempt from fulfilling requests. It ensures alignment with data protection laws and reflects internal responsibilities in processing such requests.

3. POLICY OVERVIEW

- All data subject requests must be directed promptly to the Data Controller at **privacy@kadence.co**.
- Communications with the data subject must be clear, concise, and accessible. If addressed to children, the language should be easily understandable.
- No fees will be charged for processing requests or providing access to personal data, except where requests are manifestly unfounded, excessive, or repetitive. In such cases, a reasonable administrative fee may apply.
- If a request is denied, Kadence will inform the data subject, including the reason for the denial and their right to escalate to the **Information Commissioner's Office (ICO)** or pursue legal action.

4. RESPONSE TIMES

- Requests must be answered **without undue delay** and no later than **one month** from receipt.
- For complex or multiple requests, the response period may be extended by **two additional months**. The data subject must be informed of any extension within one month.
- Kadence maintains a **register of data subject requests**, logging the type, date, and compliance deadlines to ensure accurate tracking.

5. IDENTIFICATION VERIFICATION

- If there are doubts about the identity of the requestor, reasonable steps (e.g., checking passports or driver's licenses) must be taken to confirm their identity.
- Where requests are made online, additional verification measures may be required. The response period will begin only after identity verification is completed.

6. DATA SUBJECT ACCESS REQUESTS (SARs)

Data subjects can request:

- **Confirmation** of whether their personal data is being processed.
- **Access** to their personal data and a **copy** of it.
- **Details** of:
 - The purposes of processing
 - Categories of personal data processed
 - Recipients (or categories of recipients) of the data
 - Data retention periods or the criteria used to determine retention
 - The right to rectify, erase, or restrict data processing

- Their right to lodge a complaint with the **ICO**
 - Data sources (if data was not collected directly)
 - Any automated decision-making, including profiling
 - Data transfers outside the **European Economic Area (EEA)**, including applicable safeguards.
- Responses to SARs sent via email will generally be provided electronically, with appropriate **encryption** for data security unless otherwise requested.

Third-Party Data

Personal data relating to third parties will not be disclosed without:

1. **Consent** from the third party, or
2. **Reasonable justification** to disclose it without consent, considering:
 - The type of data
 - Any confidentiality obligations
 - The efforts taken to obtain consent
 - Whether the third party can provide consent
 - Any explicit refusal by the third party.

7. RECTIFICATION OF PERSONAL DATA

Data subjects can request the correction of **inaccurate or incomplete personal data**.

- Kadence will rectify the data **without undue delay** across all data locations and formats to ensure consistency.
- If personal data was shared with third parties, those third parties will also be notified of the rectification unless doing so is impossible or requires disproportionate effort.
- The data subject will be informed of the rectification.

8. ERASURE OF PERSONAL DATA (“Right to be Forgotten”)

Data subjects can request deletion of their personal data if:

- The data is no longer necessary for its original purpose.
- Consent for processing has been withdrawn.
- The data subject objects, and no overriding legitimate grounds exist.
- Processing is unlawful or lacks a legal basis.
- There is a legal obligation to erase the data.

Kadence will erase relevant personal data from all sources and locations. If the data has been made public, reasonable steps will be taken to inform other controllers to delete it.

Exceptions include where processing is required for:

- Legal compliance, public interest, or official authority.
- Establishment, exercise, or defense of legal claims.

9. RESTRICTION OF PROCESSING

Data subjects can request restriction of processing in the following cases:

- The accuracy of the data is contested, pending verification.
- Processing is unlawful, and the data subject opts for restriction instead of erasure.
- Kadence no longer needs the data, but the subject requires it for legal claims.
- The data subject has objected, and verification of legitimate interests is pending.

Restricted data may only be processed with the subject’s consent or for legal reasons. If the restriction is lifted, the data subject will be informed.

10. DATA PORTABILITY

Data subjects can request a copy of their personal data in a **structured, commonly used, and machine-readable format** to transfer to another data controller if:

- The legal basis for processing is **consent** or **contractual necessity**.
- The data is processed through **automated means**.

Kadence will assist with direct data transfer where technically feasible.

11. OBJECTION TO PROCESSING

Data subjects can object to processing if:

- It is based on **legitimate interests** that do not override their rights and freedoms.
- The data is used for **direct marketing** purposes.

Kadence will cease processing unless it demonstrates compelling legitimate grounds that override the data subject's interests or the data is required for legal claims.

12. AUTOMATED DECISION-MAKING AND PROFILING

Data subjects can object to **automated decision-making** that significantly affects them.

Exceptions apply if the decision:

- Is necessary for entering or performing a contract.
- Is authorized by law.
- Is based on **explicit consent**.

Where automated decisions are made, the data subject can request **human intervention**, express their point of view, and contest the decision.

13. MONITORING AND REVIEW

This policy will be **reviewed annually** or sooner if required by regulatory changes. The next review is scheduled for **October 2025**.

APPENDIX 1: EXEMPTIONS

Kadence may decline a data subject request under the following circumstances:

- **Legal privilege/confidentiality** (e.g., solicitor-client communications).
- **Non-disclosure agreements or commercial contracts** if compliance would breach confidentiality.
- **Self-incrimination** (if compliance would reveal evidence of an offense).
- **Corporate finance transactions** under certain conditions.
- **Management forecasts** where disclosure would prejudice business interests.
- **Negotiations** with the data subject.
- **Confidential references** provided by Kadence.

FINAL REMARKS

This policy ensures that Kadence complies with GDPR, the Data Protection Act 2018, and relevant privacy regulations such as the **CCPA** where applicable. It reflects Kadence's commitment to transparency, accountability, and protection of data subjects' rights.