Kocho

BECOME GREATER

Data Protection Policy

Document Version 5.0

Contact

Phone: 0800 044 5009
Email: hello@kocho.co.uk
Website: kocho.co.uk

Confidentiality

This document is classified as CORPORATE OFFICIAL and can be distributed outside of Kocho. This document and its contents are provided AS IS without warranty of any kind. All trademarks are the property of their respective companies. The names of actual companies and products mentioned may be the trademarks of their respective owners.

Identification

File Name	Owner
Data Protection Policy	Group DPO

Preparation & version tracking

Version	Role	Date	Action/comment
0.1	Information Security Manager	15/06/2021	Previously separate ThirdSpace and TiG Data Protection Policies combined into new corporate template
1.0	Information Security Manager	25/06/2021	Issue 1 approved by the Group DPO
2.0	Information Security Manager	02/11/2021	Annual review: minor updates to reflect changes in team names and roles
2.1	Information Security Manager	21/04/2022	Re-templated into Kocho template
3.0	Head of Compliance	09/12/2022	Annual review: Textual changes to improve clarity
4.0	Head of Compliance	10/11/2023	Annual review: → Text revised to enable the document to be reclassified for external distribution
5.0	Compliance Officer	13/11/2024	Annual review: A section on Data Masking will be added in due course.

Reviewers/Authorisers

Role	Reviewer/Authoriser	Date	Date of Next Review
Group Data Protection Officer	Approver	13/11/2024	November 2025

Contents

1 Introduction

Kocho recognises its obligations under the Data Protection Act 2018 (DPA) and in particular the importance of respecting the personal privacy of all its employees and the need to build in appropriate safeguards regarding the use of personal data.

This Policy uses the term 'employee' for ease of reading, and this refers to all full-time employees, agency workers and consultants. The Policy explains how Kocho will hold and process their information, their obligations as an employee with regard to data protection during their employment or engagement with Kocho, and their rights as a 'data subject' in relation to their employment or engagement.

This Policy is not contractual and may be amended at Kocho's absolute discretion.

2 Personal Data

2.1 What is 'Personal Data'?

Personal Data is data that relates to a living individual who can be identified from the data and includes any expression of option about the individual and any indication of intention in respect of that individual. It does not include data that has been anonymised.

Kocho holds personal data about employees, including:

- Recruitment information;
- Email systems;
- Electronic and paper HR files;
- Time keeping records.

Personal data may be provided to Kocho by an employee but may also be provided by third parties (such as former employers), or may be created during the employment relationship (e.g. appraisal records) or on termination (e.g. references provided to prospective employers).

2.2 Special Category Data and Data Relating to Criminal Convictions or Offences

Special category data is information relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union memberships;
- Genetic or biometric data;
- Health, details of sex life, or sexual orientation.

Kocho may collect information from an employee relating to some of these matters but will usually do so in an anonymised way. Where this is the case it will not be considered personal data. However, where the data has not been anonymised, this will be considered special category data and treated as such.

Details of any special category data Kocho may collect and process about an employee will be explained to them at the time the data is collected.

Kocho does not currently process any personal data relating to criminal convictions or offences.

2.3 Processing of Data

'Processing' means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data. It applies to a comprehensive range of activities including the initial obtaining of personal information, the retention and use of it, access and disclosure, and final disposal.

2.4 Privacy by Design

Privacy is central to data protection law and therefore Kocho will investigate the risks to employees of processing personal data, minimise those risks wherever possible, use appropriate methods to process data and ensure that processing is secure.

3 Company Confidential Data

Company confidential data is information that is not personal data. It includes, but is not limited to, information such as:

- Financial information – e.g. management accounts, budget, revenue, profitability and salary information;
- Operational information – e.g. pricing and business process information;
- IP – e.g. coding for a proprietary piece of software;
- Information relating to IT architecture – e.g. network diagrams and server addresses.

This kind of information may be owned by Kocho, its clients or suppliers. It is standard practice for the exchange of information between Kocho and its clients or suppliers to be subject to a Non-Disclosure Agreement (NDA). Such information should only be shared within Kocho with those people who have a 'need to know'. For Kocho's information, this is likely to be a wider group of people than for information that is received from a client or supplier. In any case, all employees are required to handle company confidential information of clients and suppliers with the same care for its confidentiality as would be applied to Kocho information.

4 Data Protection Principles

Kocho processes personal data in accordance with the six data protection principles, which set out that personal data shall be:

- Processed lawfully, fairly and transparently;
- Collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which processed;
- Accurate and in date and any inaccurate data rectified or erased;
- With regard to the reasons for processing, not kept for any longer than is necessary;
- Processed in a way that ensures appropriate security.

5 Lawful Processing

In line with the data protection principles, Kocho only processes personal data and special category data for the reasons notified to employees and in accordance with Kocho's obligations. Under the DPA, Kocho must have a specified, lawful basis for processing personal data.

Kocho processes personal data where necessary to manage the employment relationship, where the main lawful bases for processing employee data are:

- To comply with legal obligations (e.g. paying tax);
- To comply with contractual obligations (e.g. paying an employee according to the rate agreed);
- Because it is necessary for Kocho's legitimate interests (e.g. to manage succession planning).

Where one of these reasons applies Kocho may process an employee's data without their consent. An employee may choose not to provide certain data but by doing so this may prevent Kocho from complying with its legal obligations and may in turn affect their employment.

Where Kocho processes special category data this is only done where one of the lawful reasons set out above applies and where either:

- The employee has given consent; or
- Processing is necessary under employment law; or
- Processing is necessary to protect the employee's or another's personal vital interests and the employee is capable of giving consent; or
- The employee has made the data public; or
- Processing is necessary to do with a legal claim; or
- It is necessary for medical reasons or for the assessment of the employee's working capacity.

Where Kocho intends to process special category data relating to an employee, Kocho will explain this and set out the reasons why at the time.

6 Employee Rights as a 'Data Subject'

An employee:

- Has the right to be told what data Kocho processes, how this processing takes place and on what basis;
- Has the right to see their own personal data by making a subject access request;
- Has the right to receive a copy of their personal data and in some circumstances have their personal data transferred to another data controller, usually within a month and without charge;
- Can correct any inaccuracies in their personal data;
- May ask Kocho to erase personal data where it is no longer necessary to process it for the purpose it was collected, or where it should not have been collected;
- May object to data processing where Kocho is relying on a legitimate interest to do so and the employee thinks their rights and interests outweigh Kocho's;
- Will be notified if there is a data security breach involving their data;
- Has the right not to consent, or to withdraw their consent, to processing where the employee is relying on consent as the lawful reason to process personal data;
- Has the right to complain to the Information Commissioner. Contact details can be found on their website www.ico.org.uk

7 Subject Access Requests

All employees have the right to review the information Kocho holds about them, with some exceptions. An employee should contact the People Team if they wish to make a subject access request.

No charge will be made for a response to a subject access request.

If an employee receives a subject access request they should immediately re-direct this to the People Team.

8 Data Security and Employee Obligations

Access to employee data will be restricted to those users with a specific and legitimate business need for the data. Employees with access to personal data pertaining to other employees or clients are required to familiarise themselves with this Policy, including the data protection principles and how to comply with them.

All employees have obligations in regard to handling data at work, specifically:

- They must keep their own personal data up to date and locked away;
- They must keep all data secure through the use of strong passwords and always locking their device when not in use;
- They should only access data they are authorised to;
- They should destroy copies of personal data they create;
- They should not share personal data with anyone not authorised to see that personal data and should consider at all times whether there is a way to share data that may disclose less information, e.g. anonymising it;
- They must not store personal data on personal devices, and printed copies must not be removed from Kocho premises unless there is specific authorisation to do so;
- They must not share personal data with sources external to Kocho unless authorised to do so;
- They must not transfer personal data outside the European Economic Area (EEA) unless this has been authorised in advance;
- If they become aware of a possible data breach, however minor, this must be immediately reported to the Group Data Protection Officer (DPO).

9 Monitoring

Kocho monitors use of its systems including emails. If any other monitoring is being considered, employees will be advised of this and given all the relevant information.

10 Data Handled by a Third Party

Where employee data is transferred to a third party (e.g. for references), Kocho still retains responsibility for the secure and appropriate use of that data. Before employee data is transferred to any third party, Kocho ensures that the third party has security measures in place to protect the processing of the data.

11 Privacy Notices

Whenever Kocho collects information from an employee, is provided with information about an employee, or is planning to pass employee information to a third party, Kocho will provide employees with a privacy notice giving clear information about how and why their data is being used, where it comes from, and where it goes.

This section gives an overview of the data collected and used by Kocho in the course of its relationship with an employee. As an employer, Kocho needs to process an employee's personal data during their recruitment, employment, and following termination of employment.

This data will be used for selection, checking the right to work in the UK, administering the ongoing contract between Kocho and the employee, managing performance and conduct, making reasonable adjustments for any relevant disabilities, making salary payments, and deducting tax and national insurance. Specifically:

- Name and date of birth;
- Address, telephone number and personal email address;
- Identification documents and information about immigration status;
- National Insurance number and details of tax status;
- Information about previous employment history;
- Qualifications and professional memberships;
- Job title and place of work;
- Information about the employment contract including start date, working hours, salary and benefits;
- Gender, marital status and details of any dependents;
- Details for an emergency contact;
- Information about performance including appraisal records;
- Details of any training received;
- Details of any grievances raised or in which the employee was involved;
- Disciplinary records including investigations and warnings;
- Attendance records;
- Where appropriate, images from CCTV systems;
- Records of any correspondence between Kocho and the employee about their employment including, for example, letters confirming any change to the contract of employment.

The information will be retained by Kocho in line with data retention timescales.

12 Retention Periods

12.1 Employee Personal Data

Kocho holds and processes personal data in respect of its employees for the purposes of running its business. It is required to collect and hold personal data so that it may, for example, process payroll payments, and meet its statutory obligations. This personal data is handled solely within the Finance and People teams. It is retained during the period that an employee remains with Kocho.

Personal data that is recorded by Kocho in the course of a recruitment process is retained for 3 months and then destroyed, in case of any claim arising from the recruitment process. Personal data used for payroll processing and retained within the payroll system is retained for 6 years, in line with accounting and HMRC requirements.

When an employee leaves Kocho, that person's file is reviewed and all personal data is destroyed where it is no longer relevant, such as the individual's emergency contact details, previous addresses, or death-in-service beneficiary details. All other data is retained for a period of 2 years and then destroyed. However, where the circumstances of an employee's departure from Kocho are such as to make it more than normally likely that an employment related matter might arise in respect of that employee (for example, a claim being brought against Kocho), the data is retained for a further 4 years (making 6 years in total). The People Director must approve this extended retention period, and such extended retention will be exceptional.

12.2 Client Data

Kocho does not store or otherwise retain any client personal data. Information is stored in respect of the business relationship with the client, such as contracts, work orders and other commercial information, and client project-based information, such as project plans, workshop outputs and network and system design documents.

Contractual and commercial information is retained for 6 years to meet HMRC requirements and to facilitate a continuing business relationship with the client.

Project related information is retained for 2 years after completion of the project. At the end of the 2 years, the information is reviewed and either destroyed, or retained for a further period of 2 years where Kocho has an ongoing relationship with the client, or the prospect of a resumption of that relationship, such that the information held is considered likely to have continuing value.

12.3 Other Data

Kocho also holds other data, primarily to do with supplier contracts and relationship management, and with technical research and briefing materials. This data does not constitute personal data.

It is retained during the length of the relationship with the supplier. When that relationship terminates, the data is destroyed unless it is regarded as useful to the business, in which case it is retained. Technical research and briefing materials are retained for as long as it is considered useful to the business.

All such data is reviewed at least annually, and data that is no longer relevant to or useful in the business is destroyed.

13 Breaches of this Policy

An employee found to be in breach of this Policy will be liable to disciplinary action up to and including, in cases of a serious or deliberate breach, summary dismissal for gross misconduct.

14 Further Information

Group DPO	Email
Jacques Fourie – Global Operations Director	dpo@kocho.co.uk

15 Appendix A: Statutory Retention Periods

Record	Statutory Retention Period	Statutory Authority
Accident books, accident records/ reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163)
Accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744)
Medical records and details of biological tests under the Control of Lead at Work Regulations 1998	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543)
Medical records as specified by the Control of Substances Hazardous to Health Regulations 1999	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 (COSHH) (SI 1999/437)
Medical records under the Control of Asbestos at Work Regulations 1987and 1998 medical records containing details of employees exposed to asbestos medical examination certificates	40 years from the date of the last entry 4 years from the date of issue	The Control of Asbestos at Work Regulations (SI 1987/2115, SI 1992/3068 and SI 1998/3235)
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years	The Ionising Radiations Regulations 1999 (SI 1999/3232)
Records of tests & examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations 1999	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 (COSHH) (SI 1999/437)
Records relating to children	Until the child reaches the age of 21	Limitation Act 1980
Records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to	6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Record	Statutory Retention Period	Statutory Authority
incapacity, pension accounts and associated documents		
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
Wage/salary records (also overtime, bonuses, expenses)	3 years after the end of the tax year to which they relate	Taxes Management Act 1970

Recommended retention periods (i.e. where no statutory retention periods exist):

Record	Recommended Retention Period
Actuarial valuation reports	Permanently
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently
HMRC approvals	Permanently

BECOME GREATER
KOCHO.CO.UK

About Kocho

At Kocho, we believe greatness lies in everyone.

That's why we exist, to help ambitious companies realise their potential.

By combining the power of Microsoft cloud technology with world-class identity, cyber security and our team of talented people, we take our clients on a journey of secure cloud transformation.

And we're with you every step of the way. Because the path to greatness isn't walked alone. We help you adopt and embrace the right technology solutions at the right time.

The result? Sustainable and secure growth that amplifies your business success.

Kocho. Become Greater.

Kocho

Microsoft
Solutions partner

Think greater.

Better together.

Do what's right.

hello@kocho.co.uk

0800 044 5009