Group Data Protection Policy

September 2026

ZIGUP

Policy Details

Group Policy Name:	Group Data Protection Policy
Group Policy Owner:	Group Company Secretary
Group Policy Custodian:	ZIGUP Plc DPO
Effective Date:	September 2026
Next Review Date:	August 2027
Policy Version Number:	v3
Internal or External Use:	Internal & External
Policy Level	1

1. Policy Statement

1.1 Who We Are

ZIGUP plc ('ZIGUP' 'We', 'Us' or 'Group') and each of its group undertakings exists to keep customers mobile. We are the leading supplier of integrated mobility solutions and automotive services to a wide range of businesses and customers.

1.2 Why This Policy Is Important to Us

This Policy is a cornerstone of effective governance and risk management, as well as a driver of continual improvement in what we do, and how we do it.

It provides a framework for ensuring that we meet obligations under the data protection law.

1.3 Who This Policy Applies To

This Policy applies to all colleagues where they are acting on behalf of ZIGUP, whether engaged on a permanent or temporary basis as an employee and in addition to any external contractors, agency workers or third parties. It applies to the processing of personal data carried out by the group undertaking.

1.4 Policy Breaches

All colleagues must adhere to this policy and avoid any actions that undermine our commitment to responsible governance.

1.5 Our Commitments

- We are committed to transparent, lawful and fair processing of personal data. This includes all personal data we collect about customers, clients, colleagues and those who interact with us.
- We publish and maintain privacy notices for our customers, clients, colleagues and applicants seeking employment.
- We require all colleagues to undertake mandatory training on data protection and information security on induction and on an annual basis.
- We assess whether we need to report breaches to the supervisory authority and take appropriate action to make data subjects aware if needed.
- We provide adequate resource to ensure colleagues handle individual information rights requests within statutory deadlines.
- We assess processing of personal data considered to be high risk via a Data Protection Impact Assessment.
- We produce policies and offer guidance on data protection and information security that we communicate to colleagues.
- Our legal department oversee that our contracts are compliant with the requirements of the data protection legislation.

1.6 Keeping This Policy Up to Date

This Policy will be reviewed annually, or if the need for an ad hoc review is identified e.g., a change in legal or regulatory requirements, or, where we identify improvements in how we are delivering good outcomes for customers.

2. Policy Requirements

2.1 Definition of personal data

Personal data includes any information relating to an identified or identifiable living person.

Some personal data is more sensitive and requires more protection, this relates to information relating to:

- Race or ethnicity;
- Religious or philosophical beliefs;
- Political opinions;
- Genetic data:
- Trade union membership;
- Sexual life and sexual orientation;
- Biometric data;
- Health data;
- Criminal offences and conviction data.

2.2. Legal Obligations

Each ZIGUP group undertaking must:

- comply with the data protection legislation and the six principles under the General Data Protection Regulation to ensure that personal data is:-
    - processed fairly, lawfully and transparently;
    - used only for limited, specified purposes;
    - adequate, relevant and not excessive;
    - accurate and where necessary kept up to date;
    - not kept for longer than necessary;
    - kept secure and safe.

- Be able to evidence their compliance with the above principles in line with the accountability principle in the data protection legislation.

2.3 Record Keeping, Data Mapping and Information Asset Owners

Most organisations must document their data processing activities to some extent.

ZIGUP group undertakings with more than 250 employees must document all their personal data processing activities in a record of processing activities (ROPA). For ZIGUP group undertakings with more than 250 employees, a ROPA template is available from the Policy Custodian.

Each ZIGUP group undertaking and group function must assign an Information Asset Owner (IAO). The IAO is responsible for completing regular information audits, or data-mapping exercises, to document what personal data the group undertaking holds and where it is stored.

IAOs must be able to document:

- what personal information is held within their group business;
- where personal information is stored, ensuring that records of processing activities are compiled and maintained to enable privacy notices to be reviewed and updated;
- how the information is properly protected;
- who has access to the personal information and why;
- the retention period applicable to the personal data.

3. Training and Awareness

To ensure colleagues understand and can meet their obligations under this Policy, it is a requirement for all colleagues to complete data protection training on induction and on an annual basis.

4. Supporting and Related Documentation

Colleagues have access to additional policies and guidance on the intranet to support the application of the data protection legislation, this includes:

- Group DPIA guidance on when to complete a DPIA, template screening questions and template DPIA.
- Group guidance on handling subject access requests.
- Group guidance on personal data breaches.
- Group data record retention policy.
- Group information security incident management policy.
- Group information security policy.
- Group acceptable use policy.

5. Declaration

The contents of this Policy have been consulted and considered with identified interested parties as identified by the Group Policy Owner.

This a **Level 1** Group policy. The content and commitments of this Policy have been reviewed by the Executive Committee ahead of final approval by the Group plc board on 29th September 2026

The content and commitments of this Policy is hereby signed off by the Company Secretary on 29th September 2026.