



excelerated Privacy Statement

Issue Date

30 JUN 2026

Contents

1	Introduction	2
2	Security	2
3	Categories of personal data we collect	3
4	Business Contacts	3
4.1	Use of Personal Data	4
4.2	Data Retention	4
4.3	Sharing and processing locations	4
5	Corporate Clients (and associated individuals)	4
6	Individuals whose data we process in providing services	5
7	Recruitment Services	5
8	Suppliers	6
9	Website visitors	6
10	Your Privacy Rights	6
11	Data Protection Lead	8
12	Supporting Policies	8

1 Introduction

excelerated is committed to protecting personal data. This Privacy Statement explains how and why we collect, use, disclose and protect personal data and describes the rights available to individuals.

It applies to personal data provided to us directly or obtained from third parties in connection with our business activities, including B2B marketing, client service delivery, operation of the PIIP application, recruitment, supplier management and website operation.

“excelerated”, “we”, “us” or “our” refers to the following companies (together, the “excelerated Group”):

- **Excelerated Procurement Solutions Ltd** (167-169 Great Portland Street, 5th Floor, London, W1W 5PF, United Kingdom)
- **Excelerated Procurement Solutions Inc.** (2nd Floor, 1345 Avenue of the Americas, New York, NY 10105, United States of America)
- **Cordis Solutions Ltd** (167-169 Great Portland Street, 5th Floor, London, W1W 5PF, United Kingdom)

Personal data means any information relating to an identified or identifiable individual. When we refer to “you” or “your”, we mean the individual whose personal data is being processed.

We process personal data for a variety of purposes and the method of collection, lawful basis, use, disclosure and retention period may differ depending on the context.

This Privacy Statement is intended to comply with applicable privacy and data protection laws, including:

- UK GDPR and the Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)
- United States state privacy laws (including the California Consumer Privacy Act as amended by the CPRA)

We act as a data controller except where we process personal data on behalf of our clients as a service provider or processor.

2 Security

We take the security of personal data seriously. Our information security management system is certified to ISO/IEC 27001 and we maintain policies, procedures and training covering data protection, confidentiality and information security.

We regularly review our security controls to ensure that personal data is protected against unauthorised access, loss, misuse or disclosure.

3 Categories of personal data we collect

Depending on your relationship with us, we may collect:

- identifying information such as name and internal reference numbers;
- business contact information such as business email address, telephone number, employer and business address;
- professional information such as job title, department and areas of business interest;
- account and authentication information for our systems;
- technical and website usage information such as IP address, device identifiers and log data;
- marketing and communications information such as preferences and campaign interactions;
- recruitment and employment information; and
- supplier and contractor contact information.

PIIP application – high-risk personal information

Where you use our PIIP application or related services, we may also process high-risk personal information including bank account details, routing or sort codes, transaction identifiers, tax identification numbers or equivalent national identifiers, and payroll or income-related information where required.

This information is treated as confidential and protected using enhanced technical and organisational security measures.

4 Business Contacts

We process personal data about individuals we interact with during our business activities. This includes contacts at current and prospective clients, partners, advisers, suppliers and other organisations.

We collect this information directly from you, from your employer or organisation, from our clients, from publicly available sources (such as professional networking platforms), and from third-party providers such as business development or recruitment databases.

The information typically includes name, business contact details, job title, employer and areas of professional interest.

We use a customer relationship management system (CRM) to manage this information. The CRM may also capture limited information from our email and calendar systems relating to interactions with business contacts.

Business contact information may be shared within the excelerated Group where necessary for service delivery, software development, system support, security, compliance, internal administration or client relationship management.

4.1 Use of Personal Data

We use business contact information for the following purposes:

Administering, managing and developing our business and services

Including managing relationships, improving services, operating IT systems, hosting meetings and events, performing analytics and maintaining our websites and applications.

Conducting corporate research and market analytics

Including surveys, profiling and market analysis to improve our services.

Providing information about us and our services

Including sending communications about our professional services and business activities.

These activities are carried out on the basis of our legitimate business interests.

4.2 Data Retention

Business contact information is retained in line with our retention schedule and may be kept longer where required by law or to establish or defend legal rights.

4.3 Sharing and processing locations

We may share personal information within the excelerated Group for the purposes described in this Privacy Statement and in accordance with applicable law.

Our CRM data is hosted in North American data centres. We may also share personal data with business partners where required to deliver joint services.

We do not sell personal information under US privacy laws. Where information is shared for targeted B2B marketing activities, individuals are provided with appropriate opt-out rights where required by law.

5 Corporate Clients (and associated individuals)

We collect only the personal data necessary to provide agreed services and ask our clients to do the same.

Where we process personal data to provide services, our clients are responsible for providing information to data subjects where required. In these circumstances, we

act as a data processor and process personal data only in accordance with client instructions and applicable law.

The categories of personal data typically processed include names, contact details and job information.

Use of personal data

We use this information to administer client relationships, deliver services, perform analytics, manage security and quality assurance, and provide information about our services.

The lawful basis is legitimate interests and, where applicable, legal obligation.

Data retention

Client-related personal data is generally retained for six years unless legal or contractual requirements require longer retention.

6 Individuals whose data we process in providing services

We may process similar categories of personal data when providing services to our clients, including contact details and professional information.

We use this information to deliver professional services, manage our business, ensure security and quality, and comply with legal and regulatory obligations.

The lawful basis may include legitimate interests, legal obligation, public interest or consent depending on the service.

Data is typically retained for seven years unless a longer period is required by law.

7 Recruitment Services

We collect personal data from job applicants including contact details, employment history, qualifications, references, sensitive personal data where voluntarily provided, criminal record information where required, and right-to-work documentation.

Use of personal data

We use this information to manage recruitment, assess suitability, communicate with candidates, conduct background checks, comply with legal obligations, perform recruitment analytics and make reasonable adjustments where required.

For US residents, this processing is carried out for legitimate business recruitment purposes.

Automated decision-making

Applicants are not subject to decisions based solely on automated processing that produce legal or similarly significant effects.

Data retention

Recruitment data is retained for 1 year after application unless further consent is provided.

8 Suppliers

We process business contact data of suppliers and subcontractors to manage relationships, receive services, support client delivery, operate our business, manage security and comply with legal obligations.

Processing is based on legitimate interests and legal obligations.

Supplier contact data is retained for the duration of the relationship and thereafter in accordance with our retention schedule.

9 Website visitors

We collect limited personal data from website visitors, including contact details submitted via forms or email and technical data collected through cookies and analytics tools.

We ask that visitors do not submit sensitive personal data through the website.

Use of personal data

Website data is used to respond to enquiries, provide requested information, operate and improve the website, send marketing communications (where permitted), monitor compliance with our terms and perform analytics.

We do not sell website visitor information.

Cookies

We use cookies to operate our website and improve user experience. Where required by law, we obtain consent before placing non-essential cookies. Visitors can manage cookie preferences through browser settings or our cookie banner.

Third-party links

Our website may link to third-party websites. We are not responsible for their privacy practices.

Data retention

Website data is retained only as long as necessary for the relevant purpose.

10 Your Privacy Rights

Depending on your location and the applicable data protection legislation, you may have the right to:

- access and obtain a copy of your personal data;
- request the correction of inaccurate or incomplete personal data;
- request the deletion of your personal data where applicable;
- request the restriction of processing;
- object to the processing of your personal data, including for direct marketing purposes;
- request the transfer of your personal data to another organisation (data portability);
- withdraw your consent at any time where processing is based on consent;
- opt out of the sale or sharing of personal data (where applicable under US privacy laws);
- limit the use of sensitive personal information (where applicable under US privacy laws);
- appeal decisions relating to your privacy rights requests (where applicable under US privacy laws);
- raise a complaint with us regarding how we collect, use, store or otherwise process your personal data; and
- lodge a complaint with the relevant supervisory authority where you believe your personal data has not been processed in accordance with applicable data protection legislation.

Requests relating to your privacy rights, including data protection complaints, should be submitted by email to info@excelerateds2p.com.

If you submit a data protection complaint, we will:

- acknowledge receipt of your complaint within 30 calendar days;
- investigate your concerns fairly, impartially and without undue delay;
- keep you informed of the progress of our investigation where appropriate;
- provide you with a written response explaining the outcome of our investigation and any actions we have taken.

We may need to verify your identity before responding to any request or complaint in order to protect your personal information and ensure that personal data is disclosed only to authorised individuals.

If you remain dissatisfied with our response, you have the right to lodge a complaint with the relevant supervisory authority responsible for data protection in your jurisdiction. If you are located in the United Kingdom, this is the Information Commissioner's Office (ICO). If you are located in the European Economic Area, you may also contact your local supervisory authority. Where applicable under US state privacy laws, you may contact the relevant state privacy regulator.

11 Data Protection Lead

The Data Protection Lead oversees data protection compliance for all companies within the excelerated Group.

Contact: info@excelerateds2p.com

12 Supporting Policies

This Privacy Statement is supported by our internal:

- Data Protection Policy
- Data Retention Schedule
- Information Security Incident Response Procedure
- Supplier Information Security Procedure
- ISO 27001 ISMS