Privacy Policy

Version History

Date	Version	Reason for Change	Author
02/11/2023	1.0.0	Initial Release	Naq
23/05/2024	2.0.0	Document structure changed	Tanja Martin

Privacy policy

Introduction

electroCore UK Ltd respects the privacy of its customers, suppliers and partners. We have therefore formulated and implemented a policy on complete transparency regarding the processing of personal data, its purpose(s) and the possibilities to exercise your legal rights in the best possible way. For employees, we have formulated a separate privacy policy, available upon employment and upon request.

This privacy policy pertains to processing by electroCore UK Ltd by means other than through the use of cookies. electroCore UK Ltd has formulated a separate cookie policy, which can be found on our electroCore UK Ltd's websites: https://www.gammacore.co.uk

Definitions

- Party responsible for processing personal data: electroCore UK Ltd; with registered address at Suite Ff10, Brooklands House, 58 Marlborough Road, in United Kingdom; company registration number 09432721 and Data Protection Officer Jerod Mills who can be reached at jerod.mills@elecrocore.com (the “Controller”).
- Data Protection Authority: The Data Protection Authority of United Kingdom.
- Data Protection laws:
  - For European citizens or residents, the EU GDPR 2018; the EU e-privacy directive 2002 (soon to be replaced by the EU e-privacy regulation);
  - For UK citizens or residents, the UK GDPR 2020 and the UK Data Protection Act 2018
  - and the national laws of the countries where we operate.

Collection of data

- Your personal data will be collected by electroCore UK Ltd and its data processors.
- Personal data means any information relating to an identified or identifiable natural person (‘data subject’).
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The types of personal data we may process:

Business process	Type	Data subject	Legal basis
Website	Copy of ID, National Insurance Number, Protected characteristics, Non-PII data, Bank account or creditcard number, Intellectual Property, General Health Data, Date of Birth, Photographs, Contracts, Email Address, Video, Home Address, Source Code, Educational and Employment History	Business Partners, Contractors, Customers, Employees, Patients, Suppliers	Consent
Email	Bank account or creditcard number, Contracts, Copy of ID, Date of Birth, Educational and Employment History, Email Address, General Health Data, Home Address, Intellectual Property, National Insurance Number, Non-PII data, Photographs, Protected characteristics, Source Code, Video	Business Partners, Contractors, Customers, Employees, Patients, Suppliers	Legitimate interest

Storage and exchange of documents	Bank account or creditcard number, Contracts, Copy of ID, Date of Birth, Educational and Employment History, Email Address, General Health Data, Home Address, Intellectual Property, National Insurance Number, Non-PII data, Photographs, Protected characteristics, Source Code, Video	Business Partners, Contractors, Customers, Employees, Patients, Suppliers	Legitimate interest
Delivery of goods and services	Copy of ID, National Insurance Number, Protected characteristics, Non-PII data, Bank account or creditcard number, Intellectual Property, General Health Data, Date of Birth, Photographs, Contracts, Email Address, Video, Home Address, Source Code, Educational and Employment History	Business Partners, Contractors, Customers, Employees, Patients, Suppliers	Performance of a contract
Financial and business administration	Contracts, Video, Copy of ID, Protected characteristics, Source Code, Educational and Employment History, National Insurance Number, General Health Data, Photographs, Non-PII data, Bank account or creditcard number, Intellectual Property, Date of Birth, Email Address, Home Address	Employees, Patients, Business Partners, Suppliers, Customers, Contractors	Legitimate interest
Marketing	National Insurance Number, General Health Data, Contracts, Photographs, Video, Copy of ID, Protected characteristics, Non-PII data, Bank account or creditcard number, Intellectual Property, Date of Birth, Email Address, Home Address, Source Code, Educational and Employment History	Business Partners, Contractors, Customers, Employees, Patients, Suppliers	Consent

Purposes

electroCore UK Ltd processes personal data for one or more of the following purposes:

- Customer, employee, contractor, partner or supplier management
- Business and financial administration
- Direct marketing
- Delivery of goods or services
- Work planning

How we collect, store or otherwise process your data:

The following business processes describe how we may collect, store or otherwise process the types of personal information set out in the table above:

- Collection of cookies, subscription to newsletter or filling out the contact form on the website(s);
- Analyse trends and profiles, for our legitimate interest to aim to enhance, modify, personalise and improve our services and communications for the benefit of our customers;
- Process and respond to support requests, enquiries and complaints received from you through use of business email;
- Provide services and products requested and/or purchased by you and to communicate with you about such services and/or products. We do this as necessary in order to carry out a contract with you and in accordance with our legitimate interest to operate a business;
- Carry out administrative activities such as invoicing and collecting payments either locally on devices or using cloud-services;
- Store and exchange personal information contained in documents through email and cloud-services;
- Marketing and customer acquisition through email or using cloud-services.

Sharing data with third parties

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your Personal Data outside United Kingdom. If we do, you can expect a similar degree of protection in respect of your Personal Data.

We will only share your Personal Data with third parties in accordance with the GDPR and as outlined in the

legal justification table above.

We share your personal data with the following enterprise third parties. We also share your data with SME third parties, details of which are available upon request. You will be notified when we have engaged with a new third party recipient of your personal data.

Adobe

Function	Office Management Software
Business process	Business Operations
Data categories	Non-PII data, Bank account or creditcard number, General Health Data, Date of Birth, Contracts, Email Address, Educational and Employment History
Data subjects	Contractors, Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Apple iCloud

Function	Document Storage
Business process	Storage of Digital Documents
Data categories	Photographs, Email Address, Video
Data subjects	Business Partners, Contractors, Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

AWS

Function	Application Hosting, CRM, Document Storage, Website Hosting
Business process	Business Operations, Delivery of Goods and Services, Storage of Digital Documents
Data categories	Date of Birth, Email Address, Home Address, Non-PII data, Protected characteristics
Data subjects	Customers, Employees, Patients
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

DocuSign

Function	Document Storage, Office Management Software
Business process	Business Operations, Storage of Digital Documents
Data categories	Contracts, Email Address, Non-PII data
Data subjects	Contractors, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest

	and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Calendly

Function	Appointment Scheduling Tool, Customer Service
Business process	Business Operations
Data categories	Email Address
Data subjects	Customers, Patients
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Dropbox

Function	Document Storage
Business process	Storage of Digital Documents
Data categories	Protected characteristics, Non-PII data, Bank account or creditcard number, General Health Data, Date of Birth, Photographs, Contracts, Email Address, Video, Home Address
Data subjects	Contractors, Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Google Ad Manager

Function	Marketing Tool
Business process	Marketing
Data categories	Bank account or creditcard number, Non-PII data
Data subjects	Customers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Google Analytics

Function	Marketing Tool
Business process	Marketing, Website
Data categories	Bank account or creditcard number
Data subjects	Customers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Google Workspace

Function	Office Management Software
Business process	Business Operations, Delivery of Goods and Services, Email, Storage of Digital Documents
Data categories	Protected characteristics, Non-PII data, Bank account or creditcard number, General Health Data, Date of Birth, Photographs, Contracts, Email Address, Video, Home Address, Educational and Employment History
Data subjects	Contractors, Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Mailchimp

Function	Marketing Tool
Business process	Marketing
Data categories	Email Address, Protected characteristics
Data subjects	Customers, Patients
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Microsoft Office 365

Function	Office Management Software
Business process	Business Operations, Storage of Digital Documents
Data categories	Protected characteristics, Non-PII data, Bank account or creditcard number, General Health Data, Date of Birth, Contracts, Email Address, Educational and Employment History
Data subjects	Contractors, Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Paypal

Function	Payment, Payment Processing
Business process	Business Operations
Data categories	Email Address, Home Address, Protected characteristics
Data subjects	Customers, Patients
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Salesforce

Function	CRM
Business process	Business Operations, Delivery of Goods and Services, Marketing
Data categories	Bank account or creditcard number, Email Address, General Health Data, Home Address, Non-PII data, Protected characteristics
Data subjects	Customers, Patients
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Stripe

Function	Payment
Business process	Business Operations
Data categories	Bank account or creditcard number, Email Address, General Health Data, Protected characteristics
Data subjects	Customers, Patients
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Whatsapp

Function	Office Management Software
Business process	Business Operations
Data categories	Email Address, Protected characteristics, Home Address, General Health Data
Data subjects	Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

Zoom

Function	Other Software Suite
Business process	Business Operations
Data categories	Protected characteristics, Email Address, Video
Data subjects	Contractors, Customers, Employees, Patients, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimized and regularly deleted according to national retention periods.

International data transfers

The third parties we have engaged for the abovementioned business process may transfer your personal information to outside of your jurisdiction. electroCore UK Ltd's third party processors take all necessary measures to ensure the confidentiality, availability and integrity of personal data and to comply with the GDPR with regards to international data transfers. The international nature of its compliance certifications, as well as far-reaching technical security measures (including but not limited to encryption of the personal data, making the data illegible to an unauthorised recipient) are sufficient to ensure that the data subjects continue to benefit from the fundamental rights they are entitled to under the GDPR.

Where electroCore UK Ltd transfers data to third countries, it relies on the following legal grounds for international data transfers:

- An Adequacy Decision in accordance with article 45 of the GDPR
- In the absence of an Adequacy Decision, appropriate safeguards in the form of Standard Contractual Clauses or Binding Corporate Rules.

In the event that electroCore UK Ltd is reliant on Standard Contractual Clauses for the legality of its international data transfer, it ensures that the Processor or Subprocessor takes supplementary security measures to safeguard the international data transfer with one or more of the following measures:

- Encryption;
- Anonymisation;
- Pseudonymisation.

Storage and protection of data

Your data is protected by electroCore UK Ltd and its processors in pursuance to all legal requirements set by the relevant data processing laws. electroCore UK Ltd has taken technical and organizational security measures to protect your data and requires its data processors to meet the same requirements. electroCore UK Ltd has signed processing agreements with its processors to ensure an adequate level of data protection.

The following security measures are taken by electroCore UK Ltd to protect your personal data in the course of the listed business processes:

Organisational security measures

Staff

electroCore UK Ltd staff members are required to conduct themselves in a manner consistent with electroCore UK Ltd's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. All staff members undergo appropriate background checks prior to hiring and sign a confidentiality agreement outlining their responsibility in protecting customer data.

We continuously train staff members on best security practices, including how to identify social hacks, phishing scams, and hackers.

Access controls

electroCore UK Ltd maintains your data privacy by allowing only authorized individuals access to information when it is critical to complete tasks for you. electroCore UK Ltd staff members will not process customer data without authorization.

Data hosting

As a rule, data is hosted within countries and areas that provide a substantially similar level of protection as data subjects have under the GDPR. To ensure this, we rely on Adequacy Decisions as a legal basis for our international data transfers. In exceptional circumstances, where data is transferred to a country or area not subject to an Adequacy Decision, we rely on Standard Contractual Clauses with the recipient and take supplementary security measures to secure this data transfer, such as anonymisation.

Physical security

The data centres on which personal data is hosted are secured and monitored 24/7 and physical access to facilities is strictly limited to select staff.

Technical security measures

All devices which are used to access personal data for which we are responsible are secured with antivirus

software, firewalls, encryption and access management. We regularly update operating systems and software to ensure vulnerabilities cannot be exploited.

We carry out regular vulnerability scanning of our website and have engaged credentialed external auditors to verify the adequacy of our security and privacy measures.

Your rights regarding information

Each data subject has the right to information on and access to, and rectification, erasure and restriction of processing of their personal data, as well as the right to object to the processing and the right to data portability.You also have the right to request that you are not made subject to decision making based solely on automated processes, including profiling, if these decisions would have a significant effect on you.

You can exercise these rights by contacting us at the following email address: customerserviceuk@electrocore.com. If we have any doubts as to your identity, we may request you to provide us with proof of identification, such as through sending us a copy of your valid ID. Ensure that you write “Data Request” in the subject line of your email.

Within one month of the submitted request, you will receive an answer from us. We will not charge you for submitting your request unless the request is manifestly unfounded or otherwise unreasonable in its nature. Depending on the complexity and the number of the requests this period may be extended to two months.

Marketing

- You may receive commercial offers from electroCore UK Ltd. If you do not wish to receive them (anymore), please send us an email to the following address: customerserviceuk@electrocore.com and ensure that you write “Data Opt-Out” in the subject line of your email.
- Your personal data will not be used by our partners for commercial purposes.
- If you encounter any personal data from other data subjects while visiting our website, you are to refrain from collection, any unauthorized use or any other act that constitutes an infringement of the privacy of the data subject(s) in question. The collector is not responsible in these circumstances.

Data retention

The collected data are used and retained for the duration determined by law. You may, at any time, request your data to be deleted from any electroCore UK Ltd account, system or other data processing medium in accordance with the process described above.

Applicable law

These conditions are governed by the laws and regulations of the country where we are headquartered. The court in the district where we are headquartered has the sole jurisdiction if any dispute regarding these conditions may arise, save when a legal exception applies.

Children's Data

We do not knowingly process children's data, unless specifically stated in this Privacy Policy. If you have concerns about or knowledge of a child using our services, products, websites or apps without parental consent, please contact our DPO via jerod.mills@elecrocore.com to ensure we can take appropriate action as soon as possible.

Contact

For questions about this privacy policy, product information or information about the website itself, please contact: customerserviceuk@electrocore.com.

International data transfers

Third Party Applications

Adobe

Third party headquarter address	345 Park Avenue San Jose, CA 95110-2704, United States of America

The primary location of processing is the United States of America.	Personal data collected by Adobe may be stored and processed in any country where Adobe or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Adobe's Privacy Policy	https://www.adobe.com/privacy.html

Apple iCloud

Third party headquarter address	Apple Inc. One Apple Park Way, Cupertino, California, 95014, United States of America
The primary location of processing is the United States of America.	Personal data collected by Apple iCloud may be stored and processed in any country where Apple iCloud or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Apple iCloud's Privacy Policy	https://www.apple.com/uk/legal/privacy/en-ww/

AWS

Third party headquarter address	410 Terry Ave. North, Seattle, WA, 98109-5210, United States of America
The primary location of processing is the United States of America.	Personal data collected by AWS may be stored and processed in any country where AWS or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see AWS's Privacy Policy	https://aws.amazon.com/privacy/

DocuSign

Third party headquarter address	221 Main Street, Suite 1550, san Fransisco, CA 94105, United States of America
The primary location of processing is the United States of America.	Personal data collected by DocuSign may be stored and processed in any country where DocuSign or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see DocuSign's Privacy Policy	https://www.docusign.com/company/privacy-policy

Calendly

Third party headquarter address	271 17th St NW, Ste 1000, Atlanta, Georgia, 30363, United States of America
	Personal data collected by Calendly may be stored

The primary location of processing is the United States of America.	Personal data collected by Calendly may be stored and processed in any country where Calendly or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Calendly's Privacy Policy	https://calendly.com/privacy

Dropbox

Third party headquarter address	333 Brannan Street San Francisco, CA 94107, United States of America
The primary location of processing is the United States of America.	Personal data collected by Dropbox may be stored and processed in any country where Dropbox or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Dropbox's Privacy Policy	https://www.dropbox.com/features/cloud-storage/cloud-security

Google Ad Manager

Third party headquarter address	1600 Amphitheatre Parkway in Mountain View, CA 94043, United States of America
The primary location of processing is the United States of America.	Personal data collected by Google Ad Manager may be stored and processed in any country where Google Ad Manager or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Ad Manager's Privacy Policy	https://policies.google.com/privacy?hl=en

Google Analytics

Third party headquarter address	1601 Amphitheatre Parkway, Mountain View, CA 94043, United States of America
The primary location of processing is the United States of America.	Personal data collected by Google Analytics may be stored and processed in any country where Google Analytics or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Analytics's Privacy Policy	www.google.com/policies/privacy/partners/,

Google Workspace

Third party headquarter address	1602 Amphitheatre Parkway, Mountain View, CA, 94043, United States of America
The primary location of processing is the United States of America.	Personal data collected by Google Workspace may be stored and processed in any country where Google Workspace or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Workspace's Privacy Policy	https://policies.google.com/privacy?hl=en-US

Mailchimp

Third party headquarter address	675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, United States of America
The primary location of processing is the United States of America.	Personal data collected by Mailchimp may be stored and processed in any country where Mailchimp or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Mailchimp's Privacy Policy	https://www.intuit.com/privacy/statement/

Microsoft Office 365

Third party headquarter address	1 Microsoft Way, Redmond, WA 98052-6399, United States of America
The primary location of processing is the United States of America.	Personal data collected by Microsoft Office 365 may be stored and processed in any country where Microsoft Office 365 or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Microsoft Office 365's Privacy Policy	https://privacy.microsoft.com/en-ca/privacystatement

Paypal

Third party headquarter address	2211 North First Street, San Jose, California 95131, United States of America
The primary location of processing is the United States of America.	Personal data collected by Paypal may be stored and processed in any country where Paypal or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Paypal's Privacy Policy	https://www.paypal.com/uk/webapps/mpp/ua/privacy-full

Salesforce

Third party headquarter address	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States of America
The primary location of processing is the United States of America.	Personal data collected by Salesforce may be stored and processed in any country where Salesforce or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Salesforce's Privacy Policy	https://www.salesforce.com/eu/company/privacy/full_privacy/

Stripe

Third party headquarter address	510 Townsend Street San Francisco, CA 94103, United States of America
The primary location of processing is the United States of America.	Personal data collected by Stripe may be stored and processed in any country where Stripe or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Stripe's Privacy Policy	https://stripe.com/en-gb-nl/privacy

Whatsapp

Third party headquarter address	1601 Willow Rd, Menlo Park, California, 94025, United States of America
The primary location of processing is the United States of America.	Personal data collected by Whatsapp may be stored and processed in any country where Whatsapp or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Whatsapp's Privacy Policy	https://www.whatsapp.com/legal/privacy-policy

Zoom

Third party headquarter address	San Jose, 55 Almaden Blvd, United States of America
The primary location of processing is the United States of America.	Personal data collected by Zoom may be stored and processed in any country where Zoom or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Zoom's Privacy Policy	https://explore.zoom.us/en/privacy/

Suppliers

electroCore, Inc.

Country where data is processed or sent to	United States of America
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible