Privacy Policy

Version History

Date	Version	Reason for Change	Author
09/05/2025	1.2.0	Section(s) updated: 1,2,3	Grzegorz Zysko
06/05/2025	1.1.0	Section(s) updated: 1,2,3	Sheila Smart
16/04/2025	1.0.0	Initial generation	Sheila Smart

Privacy policy

Introduction

Genedrive Diagnostics 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 Genedrive Diagnostics Ltd by means other than through the use of cookies. Genedrive Diagnostics Ltd has formulated a separate cookie policy, which can be found on our Genedrive Diagnostics Ltd's websites: https://genedrive.com

Definitions

- Party responsible for processing personal data: Genedrive Diagnostics Ltd; with registered address at The Incubator Building, Grafton Street in United Kingdom; company registration number 03901952 and Data Protection Officer Russ Shaw who can be reached at r.shaw@genedrive.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 Genedrive Diagnostics 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 through third party applications:

Business process	Data	Legal basis
Technical Drawing	Company - Intellectual Property	Legitimate Interests

Communication	Company - Intellectual Property, User Name, Video, Email Address, First Name, Last Name, Telephone Number, Photographs Customers - Email Address, First Name, Last Name, IP Address	Legitimate Interests
Product Development	Company - User Name, Intellectual Property, Email Address, IP Address, First Name, Last Name, Job Title Customers - First Name, Last Name, Email Address	Legitimate Interests
CRM	Customers - First Name, Email Address, Telephone Number	Data Subject Consent
Testing	Company - First Name, Last Name, Email Address Customers - First Name, Last Name, Email Address	Legitimate Interests
Payroll	Employees - Age or Age Group, Date of Birth, First Name, National Insurance Number, Bank account or creditcard number, Gender, Home Address, Job Title, Salary Information, Email Address, Last Name	Contract Performance
Document Storage	Company - User Name, Intellectual Property, Contracts, Job Title, First Name, Last Name, Email Address	Legitimate Interests
Office Management	Company - Intellectual Property, Email Address, First Name, Last Name, Job Title, User Name, Contracts	Legitimate Interests
AI-Powered Tool	Company - First Name, Last Name, Job Title, User Name, Intellectual Property	Legitimate Interests
Security	Company - First Name, Last Name, Email Address, User Name	Legitimate Interests
E-Signature	Company - User Name, Intellectual Property, First Name, Last Name, Job Title	Data Subject Consent
Compliance	Company - User Name, Intellectual Property, First Name, Last Name, Email Address, Job Title	Legal Obligation Compliance
Training	Company - User Name, Intellectual Property, First Name, Last Name, Email Address	Data Subject Consent
CAD	Company - Intellectual Property	Legitimate Interests
Accounting	Suppliers - Bank account or creditcard number, Email Address, Last Name, First Name	Legal Obligation Compliance
Email	Company - User Name, Contracts, Job Title, Intellectual Property, First Name, Last Name, Email Address	Legitimate Interests
Task Management	Company - First Name, Last Name, Email Address, User Name, Intellectual Property, Job Title Customers - First Name, Last Name, Email Address	Legitimate Interests
Technical Tool	Company - Email Address, IP Address, Intellectual Property, First Name, Last Name, Job Title, User Name Patients - Date of Birth, Medical tracking (e.g. blood pressure; blood values), Last Name, User Name Users - User Name	Legitimate Interests

Work Planning	Company - First Name, Last Name, Email Address Customers - First Name, Last Name, Email Address	Legitimate Interests
Marketing	Company - Intellectual Property, Email Address, First Name, Last Name, Job Title, User Name, Video, Photographs, Browser Information, IP Address Customers - Email Address, First Name, Last Name, IP Address, Job Title, User Name	Legitimate Interests

Purposes

Genedrive Diagnostics 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:

- 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.

Pipedrive

Function	CRM
Data categories	Email Address, First Name, Telephone 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.

Ideagen Q-Pulse Quality Management System

Function	Compliance, Document Storage, E-Signature, Product Development, Training
Data categories	Intellectual Property, User Name
Data subjects	Company
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.

Sage200

Function	Accounting
Data categories	Bank account or creditcard number, Email Address, First Name, Last Name
Data subjects	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.

Sage payroll

Function	Payroll
Data categories	Age or Age Group, Bank account or creditcard number, Date of Birth, Email Address, First Name, Gender, Home Address, Job Title, Last Name, National Insurance Number, Salary Information
Data subjects	Employees
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.

Bitbucket (Atlassian)

Function	Product Development, Technical Tool
Data categories	Email Address, IP Address
Data subjects	Company
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.

Confluence

Function	Communication, Document Storage, Product Development
Data categories	Intellectual Property
Data subjects	Company
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.

Jira (Atlassian)

Function	Product Development, Task Management, Testing, Work Planning
Data categories	Email Address, First Name, Last Name
Data subjects	Company, 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.

Solidworks

Function	CAD, Document Storage, Product Development, Technical Drawing
Data categories	Intellectual Property
Data subjects	Company
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 Sharepoint

Function	Marketing, Office Management, Product Development
Data categories	Email Address, First Name, Intellectual Property, Job Title, Last Name
Data subjects	Company
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	Document Storage, Email, Office Management
Data categories	Contracts, Email Address, First Name, Intellectual Property, Job Title, Last Name, User Name
Data subjects	Company
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 Teams

Function	Communication
Data categories	Email Address, First Name, Last Name, User Name, Video
Data subjects	Company
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.

Naq Cyber

Function	Compliance, Security, Training
Data categories	Email Address, First Name, Last Name, User Name
Data subjects	Company
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.

Adobe

Function	Compliance, E-Signature
Data categories	First Name, Job Title, Last Name
Data subjects	Company
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 Visio

Function	Product Development, Technical Tool
Data categories	First Name, Intellectual Property, Job Title, Last Name
Data subjects	Company
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.

Scandit

Function	Technical Tool
Data categories	IP Address
Data subjects	Company
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.

T&D graph

Function	Compliance, Technical Tool
Data categories	User Name
Data subjects	Company
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.

TR7 for windows

Function	Compliance, Technical Tool
Data categories	User Name
Data subjects	Company
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.

Visual Studio Code

Function	Product Development
Data categories	User Name
Data subjects	Company
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.

LightCycler 480 Software

Function	Product Development, Technical Tool
Data categories	User Name
Data subjects	Company
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.

QuantStudio

Function	Product Development, Technical Tool
Data categories	User Name
Data subjects	Company
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.

Applied Biosystems 7500 Real-Time PCR

Function	Product Development, Technical Tool
Data categories	User Name
Data subjects	Company
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.

CFX Maestro

Function	Product Development, Technical Tool
Data categories	User Name
Data subjects	Company
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.

Geneious

Function	Product Development, Technical Tool
Data categories	User Name
Data subjects	Company
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.

JMP

Function	Product Development, Technical Tool
Data categories	Intellectual Property, User Name
Data subjects	Company
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.

Airtable

Function	Task Management
Data categories	Intellectual Property, User Name
Data subjects	Company
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.

ESP Flash Download Tool

Function	Technical Tool
Data categories	Intellectual Property, User Name
Data subjects	Company
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.

LinkedIn

Function	Marketing
Data categories	Email Address, Job Title, Photographs, User Name, Video
Data subjects	Company
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.

X (Twitter)

Function	Marketing
Data categories	Photographs, User Name, Video
Data subjects	Company
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.

Survey Monkey

Function	Communication, Marketing
Data categories	Email Address, First Name, IP Address, Last Name
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.

Whatsapp

Function	Communication
Data categories	First Name, Last Name, Photographs, Telephone Number
Data subjects	Company
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.

AegisPOC

Function	Technical Tool
Data categories	Date of Birth, Last Name, Medical tracking (e.g. blood pressure; blood values), User Name
Data subjects	Patients, Users
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.

InfinityPOC

Function	Technical Tool
Data categories	Date of Birth, Last Name, Medical tracking (e.g. blood pressure; blood values), User Name
Data subjects	Patients, Users
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.

POCcelerator

Function	Technical Tool
Data categories	User Name
Data subjects	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.

Aqure

Function	Technical Tool
Data categories	Date of Birth, Last Name, Medical tracking (e.g. blood pressure; blood values), User Name
Data subjects	Patients, Users
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.

EKF-Link

Function	Technical Tool
Data categories	Date of Birth, Last Name, Medical tracking (e.g. blood pressure; blood values), User Name
Data subjects	Patients, Users
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.

CoPilot

Function	AI-Powered Tool, Task Management
Data categories	First Name, Intellectual Property, Job Title, Last Name, User Name
Data subjects	Company
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.

Brevo

Function	Marketing
Data categories	Email Address, First Name, IP Address, Job Title, Last Name, User Name
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.

Bluesky

Function	Marketing
Data categories	Browser Information, Email Address, First Name, IP Address, Job Title, Last Name, User Name
Data subjects	Company
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.

Fireflies

Function	AI-Powered Tool
Data categories	First Name, Intellectual Property, Job Title, Last Name, User Name
Data subjects	Company
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. Genedrive Diagnostics 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 Genedrive Diagnostics 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 Genedrive Diagnostics 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 Genedrive Diagnostics Ltd and its processors in pursuance to all legal requirements set by the relevant data processing laws. Genedrive Diagnostics Ltd has taken technical and organizational security measures to protect your data and requires its data processors to meet the same requirements. Genedrive Diagnostics Ltd has signed processing agreements with its processors to ensure an adequate level of data protection.

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

Organisational security measures

Staff

Genedrive Diagnostics Ltd staff members are required to conduct themselves in a manner consistent with Genedrive Diagnostics 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

Genedrive Diagnostics Ltd maintains your data privacy by allowing only authorized individuals access to information when it is critical to complete tasks for you. Genedrive Diagnostics 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: info@genedrive.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 Genedrive Diagnostics Ltd. If you do not wish to receive them (anymore), please send us an email to the following address: info@genedrive.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 Genedrive Diagnostics 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 r.shaw@genedrive.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: info@genedrive.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

Airtable

Third party headquarter address	799 Market Street, 8th Floor, San Francisco, CA 94103, United States of America
The primary location of processing is the United States of America.	Personal data collected by Airtable may be stored and processed in any country where Airtable 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 Airtable's Privacy Policy	https://www.airtable.com/privacy

LinkedIn

Third party headquarter address	Sunnyvale, 1000 W Maude Ave, United States of America
The primary location of processing is the United States of America.	Personal data collected by LinkedIn may be stored and processed in any country where LinkedIn 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 LinkedIn's Privacy Policy	https://www.linkedin.com/legal/privacy-policy

Pipedrive

Third party headquarter address	Mustamäe tee 3a, Tallinn 10615, Estonia
The primary location of processing is the Estonia.	Personal data collected by Pipedrive may be stored and processed in any country where Pipedrive or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Estonia
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Pipedrive's Privacy Policy	https://www.pipedrive.com/en/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

Microsoft Teams

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 Teams may be stored and processed in any country where Microsoft Teams 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 Teams's Privacy Policy	https://privacy.microsoft.com/en-us/privacystatement

Bitbucket (Atlassian)

Third party headquarter address	Level 6, 341 George Street, Sydney, Australia
The primary location of processing is the Australia.	Personal data collected by Bitbucket (Atlassian) may be stored and processed in any country where Bitbucket (Atlassian) or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Bitbucket (Atlassian)'s Privacy Policy	https://www.atlassian.com/legal/privacy-policy

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

Naq Cyber

Third party headquarter address	Vlamingstraat 4, 2712BZ, Zoetermeer, The Netherlands
The primary location of processing is the The Netherlands.	Personal data collected by Naq Cyber may be stored and processed in any country where Naq Cyber or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and The Netherlands
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Naq Cyber's Privacy Policy	https://www.naqcyber.com/policies/privacy-policy

Visual Studio Code

Third party headquarter address	One Microsoft Way, Redmond, Washington 98052-6399, United States of America
The primary location of processing is the United States of America.	Personal data collected by Visual Studio Code may be stored and processed in any country where Visual Studio Code 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 Visual Studio Code's Privacy Policy	https://privacy.microsoft.com/en-gb/privacystatement

X (Twitter)

Third party headquarter address	Market Square, 1355 Market St suite 900, San Francisco, CA 94103, United States of America
The primary location of processing is the United States of America.	Personal data collected by X (Twitter) may be stored and processed in any country where X (Twitter) 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 X (Twitter)'s Privacy Policy	https://twitter.com/en/privacy

Survey Monkey

Third party headquarter address	One Curiosity Way, San Mateo, CA 94403, United States of America
The primary location of processing is the United States of America.	Personal data collected by Survey Monkey may be stored and processed in any country where Survey Monkey 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 Survey Monkey's Privacy Policy	https://uk.surveymonkey.com/mp/legal/privacy/

CoPilot

Third party headquarter address	Microsoft Corporation, 1 Microsoft Way, Redmond, WA, United States of America
The primary location of processing is the United States of America.	Personal data collected by CoPilot may be stored and processed in any country where CoPilot 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 CoPilot's Privacy Policy	https://privacy.microsoft.com/en-gb/privacystatement

Fireflies

Third party headquarter address	5424 Sunol Blvd , Ste 10-531 Pleasanton, CA 94566, United States of America
The primary location of processing is the United States of America.	Personal data collected by Fireflies may be stored and processed in any country where Fireflies 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 Fireflies's Privacy Policy	https://fireflies.ai/privacy_policy.pdf

Confluence

Third party headquarter address	Level 6, 341 George Street, Sydney, Australia
The primary location of processing is the Australia.	Personal data collected by Confluence may be stored and processed in any country where Confluence or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Confluence's Privacy Policy	https://www.atlassian.com/legal/privacy-policy

Brevo

Third party headquarter address	106 Bd Haussmann Paris, Île-de-France 75008 FR, France
The primary location of processing is the France.	Personal data collected by Brevo may be stored and processed in any country where Brevo or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and France
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Brevo's Privacy Policy	https://www.brevo.com/legal/privacypolicy/

Solidworks

Third party headquarter address	10, rue Marcel Dassault, Paris Campus, Vélizy-Villacoublay, 78140, France
The primary location of processing is the France.	Personal data collected by Solidworks may be stored and processed in any country where Solidworks or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and France
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Solidworks's Privacy Policy	https://discover.3ds.com/privacy-policy

Scandit

Third party headquarter address	Scandit AG Förrlibuckstrasse 181 Zurich, 8005 CH, Switzerland
The primary location of processing is the Switzerland.	Personal data collected by Scandit may be stored and processed in any country where Scandit or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Switzerland
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Scandit's Privacy Policy	https://www.scandit.com/privacy/

POCcelerator

Third party headquarter address	Siemens Healthineers AG, Siemensstr. 3, 91301 Forcheim, Germany
The primary location of processing is the Germany.	Personal data collected by POCcelerator may be stored and processed in any country where POCcelerator or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Germany
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see POCcelerator's Privacy Policy	https://www.siemens-healthineers.com/en-uk/siemens-website-privacy-policy

AegisPOC

Third party headquarter address	Abbott Laboratories, 100 Abbott Park Road, Abbott Park, IL 60064, United States of America
The primary location of processing is the United States of America.	Personal data collected by AegisPOC may be stored and processed in any country where AegisPOC 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 AegisPOC's Privacy Policy	https://www.abbott.com/privacy-policy.html

InfinityPOC

Third party headquarter address	Arvid Tydéns ava 7,171, 69 Solna, Sweden
The primary location of processing is the Sweden.	Personal data collected by InfinityPOC may be stored and processed in any country where InfinityPOC or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Sweden
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see InfinityPOC's Privacy Policy	https://diagnostics.roche.com/se/sv/legal/privacy-notice.html

ESP Flash Download Tool

Third party headquarter address	Shanghai, #204, Block 2, 690 Bibo Road, China
The primary location of processing is the China.	Personal data collected by ESP Flash Download Tool may be stored and processed in any country where ESP Flash Download Tool or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see ESP Flash Download Tool's Privacy Policy	https://www.espressif.com/en/content/privacy

T&D graph

Third party headquarter address	2-7-1 Nihonbashi, Chuo-ku, Tokyo, Japan
The primary location of processing is the Japan.	Personal data collected by T&D graph may be stored and processed in any country where T&D graph or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Japan
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see T&D graph's Privacy Policy	https://tandd.com/privacy.html

TR7 for windows

Third party headquarter address	2-7-1 Nihonbashi, Chuo-ku, Tokyo, Japan
The primary location of processing is the Japan.	Personal data collected by TR7 for windows may be stored and processed in any country where TR7 for windows or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Japan
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see TR7 for windows's Privacy Policy	https://tandd.com/privacy.html

Jira (Atlassian)

Third party headquarter address	Level 6, 341 George Street, Sydney, Australia
The primary location of processing is the Australia.	Personal data collected by Jira (Atlassian) may be stored and processed in any country where Jira (Atlassian) or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Jira (Atlassian)'s Privacy Policy	https://www.atlassian.com/legal/privacy-policy

Microsoft Sharepoint

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 Sharepoint may be stored and processed in any country where Microsoft Sharepoint 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 Sharepoint's Privacy Policy	https://privacy.microsoft.com/en-ca/privacystatement

LightCycler 480 Software

Third party headquarter address	Arvid Tydéns ava 7,171, 69 Solna, Sweden
The primary location of processing is the Sweden.	Personal data collected by LightCycler 480 Software may be stored and processed in any country where LightCycler 480 Software or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and Sweden
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see LightCycler 480 Software's Privacy Policy	https://diagnostics.roche.com/se/sv/legal/privacy-notice.html

QuantStudio

Third party headquarter address	168 Third Avenue. Waltham, MA 02451, United States of America
The primary location of processing is the United States of America.	Personal data collected by QuantStudio may be stored and processed in any country where QuantStudio 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 QuantStudio's Privacy Policy	https://www.thermofisher.com/uk/en/home/global/privacy-policy.html

Applied Biosystems 7500 Real-Time PCR

Third party headquarter address	168 Third Avenue. Waltham, MA USA 02451, United States of America
The primary location of processing is the United States of America.	Personal data collected by Applied Biosystems 7500 Real-Time PCR may be stored and processed in any country where Applied Biosystems 7500 Real-Time PCR 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 Applied Biosystems 7500 Real-Time PCR's Privacy Policy	https://www.thermofisher.com/uk/en/home/global/privacy-policy.html

CFX Maestro

Third party headquarter address	1000 Alfred Nobel Drive, Hercules, California 94547, United States of America
The primary location of processing is the United States of America.	Personal data collected by CFX Maestro may be stored and processed in any country where CFX Maestro 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 CFX Maestro's Privacy Policy	https://www.bio-rad.com/en-uk/privacy

Geneious

Third party headquarter address	Biomatters, L2, 18 Shortland Street, Auckland, 1010, New Zealand
The primary location of processing is the New Zealand.	Personal data collected by Geneious may be stored and processed in any country where Geneious or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and New Zealand
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Geneious's Privacy Policy	https://www.dotmatics.com/privacy-policy

JMP

Third party headquarter address	JMP Statistical Discovery LLC, 920 SAS Campus Drive, Cary, NC 27513, United States of America
The primary location of processing is the United States of America.	Personal data collected by JMP may be stored and processed in any country where JMP 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 JMP's Privacy Policy	https://www.sas.com/en_gb/legal/privacy.html?_ga=2.212683604.1122561556.1728642771-2143428596.1728642770

Microsoft Visio

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 Visio may be stored and processed in any country where Microsoft Visio 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 Visio's Privacy Policy	https://privacy.microsoft.com/en-ca/privacystatement

Bluesky

Third party headquarter address	113 Cherry St # 24821 Seattle, WA, 98104-2205, United States of America
The primary location of processing is the United States of America.	Personal data collected by Bluesky may be stored and processed in any country where Bluesky 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 Bluesky's Privacy Policy	https://bsky.social/about/support/privacy-policy

Suppliers