Cellmark Privacy Policy

The protection of customers' personal data is a high priority for Cellmark's management. The processing of personal data, such as your name, address, email address, or telephone number will always be in line with the General Data Protection Regulation (GDPR). This guidance is designed to inform customers and prospective customers of the sort of personal data we collect, why we collect it, how we use and your legal rights in relation to this.

Cellmark has implemented a range of technical solutions to ensure the protection of personal data processed through our websites. However, should you wish to avoid sending your personal data over the Internet, you can always use alternative means, e.g. by telephone.

Definitions

Data Subject includes, but is not limited to, customers including individuals or their representatives.

Personal Information means information which identifies or is capable of identifying an individual, which includes, but is not limited to, first and last name, date of birth, an identification number, photo, company information, home or other physical address, email address, Internet Protocol (IP) address, bank details, phone number or other contact information and medical information or one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that individual. Personal Information may also include Sensitive Personal Information, as defined below.

Sensitive Personal Information means any information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. For the purposes of this Privacy Policy, Sensitive Personal Information also includes information about criminal convictions and offences.

Processing means the collection, recording, organisation, structuring, storage, alteration, retrieval, use, disclosure by transmission, or otherwise making available, erasure or destruction of your personal data.

Anonymise means that the Data Subject cannot be identified from the data.

Controller or controller responsible for the processing. Cellmark (the Company) is the Data Controller where we are responsible for determining what personal data is collected, what reasons it is required for, how it is processed and how it is stored.

Processor the Processor is an individual, or organisation which processes personal data on behalf of the controller e.g. Cellmark acts as the processor under its contract with the Child Maintenance service.

Third party is an individual, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, is

authorised to process personal data, for example Cellmark's sampling service provider Ashlee Healthcare Limited.

Consent your Consent is your agreement to allow us to "process" your personal data, it must be freely given, be informed and specific to the purpose it is required for. You can withdraw that agreement at any time.

Name and Address of the Controller

Cellmark is the "Controller" for the purposes of the General Data Protection Regulation (GDPR), our address and contact details are as follows:

The Data Controller
Orchid Cellmark Ltd
16 Blacklands Way
Abingdon Business Park
Abingdon Oxon OX14 1DY

T: 01235 528609
E: info@cellmark.co.uk
W: www.cellmark.co.uk
www.cellmarkforensics.co.uk
www.covid19.cellmark.co.uk/
www.dna-at-home.co.uk
www.greatcrestednewtedna.co.uk/

Statement of Policy

I. Company Websites, Privacy Policy and Cookie Management

Cellmark's websites can be accessed without the need to provide personal data - however, if you wish to avail yourself of our services such as requesting additional information or registering for a test, providing your personal data could become necessary – if it is required we will obtain prior consent from you.

The Company is required by certain laws to be transparent about the Personal Information it collects and processes. All Company websites should have links on their sites which inform website visitors about the Company online information practices for Personal Information. This is provided through this Privacy Policy and as well as through a cookie settings management link on each Company website.

II. Personal Information Collected

Data Subjects may be asked to provide Personal Information when using a Company website, or interacting with the Company via other channels. The Company takes steps so that, as required by applicable law, any collection of Personal Information is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The Company may collect Sensitive Personal Information. Where required by applicable law, the Company will only collect or process Sensitive Personal Information where strictly necessary based on the informed, explicit consent of the Data Subject. To the extent that the Company processes

Sensitive Personal Information obtained from background checks (e.g. criminal convictions and offences) and other Sensitive Personal Information such as health information, the Company follows applicable laws.

Under the Human tissue Act Cellmark is required to have records of individuals consenting to undergo DNA testing. Cellmark collects and uses ethnic origin data in DNA relationship and hair toxicology cases to enable it to undertake accurate statistical analyses in line with ISFG (International Society for Forensic Genetics) and UKIAFT (United Kingdom and Ireland Association of Forensic Toxicologists) guidance. For COVID-19 testing services, because it is a notifiable disease, Cellmark is required under regulation 4 of the Health Protection (Notification) Regulations 2010 to record certain donor personal data, including ethnicity, and to report this data together with the outcome of testing to Public Health England.

III. Means of Collecting Data

Business Services: For customers, suppliers, contractors, joint venture partners, third parties and other business associates working or interacting with the Company, the Company may collect Personal Information in relation to the Data Subject's contact details, including but not limited to names, email addresses and other professional information collected in the normal course of providing or purchasing services.

We would also like to be able to keep you updated with relevant information about developments in the service we offer and will provide you with the option to opt in to receive this and other promotional information.

A **Website Visitors:** For Data Subjects using a Company website, the Company may collect Personal Information, including IP addresses, from a browsing session to facilitate use of the available services. Data collected may include the browser used and which version of it, the operating system used by your computer, the website you came from, the date and time, an IP address (either of your computer or your ISP's (Internet Services Provider) access point, and the pages you visit on our websites. Under the EU data retention directive, they are required to record such data for at least six months.

If you use our websites' contact forms or choose to register online for our testing services we will need to collect some personal data. This data is collected and stored exclusively for the purpose it was requested. We may need to transfer that data to a third party (for example our contracted sampling service) for legitimate business purposes to enable them to perform the services we have contracted with them to provide. Your details will be processed in each case in strict confidence and we will take all reasonable steps to ensure that any third party has appropriate security measures in place.

B **Cookies:** Like many other websites Cellmark's are designed to work with cookies. Cookies are text files that are stored on your computer by the Internet browser you use to access the Internet.

They have a unique ID which allows our websites to recognise individual visitors. By using cookies Cellmark can enhance the experience for visitors by tailoring the information and any offers on our websites to the individual. One example is to allow returning customers to access any private areas

of the websites more conveniently.

You will be asked if you accept the storing of cookies on your computer when you first visit our websites. You can, by changing your browser's settings, change this at any time and delete these cookies, however you may find that some functions of our website may not work properly after you have deleted them. You can also manage your acceptance of cookies at any time by clicking the cookie setting icon at the bottom of any of Cellmark's website pages.

IV. Data Protection and Social Media

Cellmark has a range of social media accounts including Facebook, Twitter, LinkedIn and Youtube. Cellmark has integrated components of services on our websites.

If you are logged in at the same time on your social media account, it will detect your activity on our website. This information is collected through "javascript" code on our websites and is linked to your social media account. If you click on one of the social media buttons integrated into our website, e.g. the "Like" button, or submit a comment, then this information is stored by the social media company and linked to your account.

The relevant data protection guidelines can be found via these links:

Facebook, https://facebook.com/about/privacy/

Twitter, https://twitter.com/privacy?lang=en

LinkedIn, https://www.linkedin.com/legal/privacy-policy

YouTube, https://www.google.com/intl/en/policies/privacy/,

V. Data Protection and Google Analytics, Google Adwords and Ruler Analytics

Cellmark employs both the Analytics and Adwords services provided by Google. Google Analytics is a web analytics service that collects data about the website from which a person has come, which other pages on the site were visited, how often and for how long a page was viewed. Google AdWords is a service for internet advertising that allows Cellmark to place ads in Google search engine results and the Google advertising network which are designed to promote our service and encourage people to visit our websites.

Google uses the data to evaluate the use of our website and to provide us with online reports which show activity across our websites, and to carry out analysis of our internet advertising.

As part of this process Google places cookies on your computer and your browser will automatically submit data to Google such as your IP address. Personal data is stored by Google outside of the EU in the USA and Google may pass this data on to third parties. Google provides detailed instructions on how to block cookies:

https://support.google.com/accounts/answer/61416

Google's privacy policy: https://www.google.co.uk/policies/privacy/

If you opt-in to cookies on our websites Cellmark will use Ruler Analytics software to collect information for marketing purposes, this information will be deleted after 6 months.

VI. Data Protection and Payments

We use PayPal and ePDQ to process payments. On our websites we offer the option to pay for our services using PayPal, which is a global online payment service provider. ePDQ is a payment solution provided by Barclays plc. which we use when we take your payment over the telephone.

The PayPal code on our website will transfer you to their website. PayPal will collect personal data, potentially including credit/debit card details, authenticate the transaction and then provide us with your (non-financial) personal data so we can continue to provide you with our testing services. When you pay for our services by telephone we will collect certain personal data including credit/debit card details which we will transfer to ePDQ to authenticate the transaction.

PayPal's privacy policy: https://www.paypal.com/us/webapps/mpp/ua/privacy-full.

ePDQ's privacy policy: https://www.barclaycard.co.uk/business/privacy-and-cookie-policy

Where we invoice you, as a VAT registered organisation, for our services we are required by HMRC (Her Majesty's Revenue & Customs) to keep your basic personal data (name, address, bank account and contact details) for a minimum of 6 years after which time it will be destroyed.

VII. Data Processing Purposes and Information Use

The Company processes Personal Information only when it has appropriate lawful grounds for doing so. Such lawful grounds may include:

- the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- the processing is necessary to comply with a legal obligation to which the Company is subject;
- the processing is within the legitimate business interests of the Company which do not outweigh the rights and freedoms of the Data Subjects;
- the consent of the Data Subjects; and
- as otherwise permitted by applicable law.

The Company will rely on consent as a lawful ground of processing only when no other lawful ground is available and will ensure that any consent collected meets the standards of valid consent under applicable law and is properly recorded**.**

VIII. Sharing of Personal Information

Sometimes the Company may need to share a Data Subject's Personal Information with its subsidiaries, affiliates, and third parties for the purposes of conducting business activities.

For example, where Cellmark has been requested to arrange sampling, or to send out a sampling kit for a sample to be taken, Cellmark will share the Data Subject's Personal Information with the third party sampler as necessary so that the sampling can be carried out.

Personal Information may be shared in the reporting of test results in accordance legitimate business processes and as defined in Cellmark's Terms and Conditions. For example Cellmark is required under regulation 4 of the Health Protection (Notification) Regulations 2010 to report

certain donor personal data with the outcome of testing to Public Health England.

The Company does not disclose Personal Information to third parties for any use that is inconsistent with this Privacy Policy. Where the Company receives Personal Information from its subsidiaries, affiliates or other entities, the Company will use such Personal Information in accordance with, as applicable, the notices provided by such entities and the choices made by the Data Subjects to whom such Personal Information relates or as otherwise permitted by applicable law.

The Company may share Personal Information about Data Subjects for the following purposes:

- if required to do so by law or legal process;
- to law enforcement authorities or other government officials, as required to comply with a legitimate legal request;
- when the Company believes disclosure is necessary to prevent physical harm, death, serious injury or financial loss;
- to protect the Company's rights and property and the rights and property of others; and
- in connection with an investigation on a matter, including suspected or actual illegal activity in which any record or other evidence of potentially illegal activity may be provided to legal authorities.

The Company reserves the right to share and transfer any Personal Information about a Data Subject to potential and subsequent business and merger partners in the event the Company sells or transfers all or a portion of its business or assets (including through merger or bankruptcy). The Company will then be responsible for requiring that such third parties have in place a privacy policy consistent with this Privacy Policy or those third parties otherwise agree in writing, to treat such Personal Information in accordance with all applicable laws.

IX. Service Provider Management

The Company may need to share certain Personal Information with the service providers it has retained to perform certain services. Where the Company engages a service provider to process any Personal Information on its behalf, the Company will adhere to its due diligence process for the selection of the service provider. This due diligence process will, amongst other things, address selected service providers' guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of applicable law.

Specifically, where required by applicable law, the Company will require that written contracts are in place with any service providers that process Personal Information on its behalf which requires the service provider to:

- act only on the Company's instructions when processing any Personal Information;
- put in place appropriate technical and organisational security measures to safeguard the Personal Information it processes on behalf of the Company, in accordance with the Company's security policies including confidentiality obligations imposed on the service provider's personnel;

- respect certain conditions when engaging sub-contractors;
- assist the Company in dealing with Data Subject's rights and in complying with the Company's obligations to the extent required under applicable legislation;
- delete or return all Personal Information processed on behalf of the Company at the end of the provision of the services;
- allow the Company to carry out data protection audits on the service provider.

X. Data Protection Impact Assessments

Where required by applicable law, the Company will assess the impact of any new processing of Personal Information that involves high risks to the rights and freedoms of Data Subjects in accordance with its data protection impact assessment process, as updated from time to time.

Where the Company does initiate new processing activities involving Personal Information, it will ensure that such processing activities conform to the requirements of applicable data protection law.

XI. Individuals' Rights

The Company will investigate and address requests to exercise individuals' rights over Personal Information in accordance with this Privacy Policy and applicable law.

- to know the reason we need to hold your personal data;
- to identify what personal data we hold;
- have we have passed on your personal data, and if so to whom – including if that has been to another country/outside of the EU and if so what safeguards are in place;
- how long your personal data will be stored;
- how to correct or update personal data that we hold;
- if we collected your personal data from another source, what was that source;
- the right to withdraw your consent for us to use your personal data at any time;
- the right to be given a copy of your personal data in a commonly used and machine-readable format
- the right to be forgotten - to have your personal data erased, promptly.

XII. Retention and Destruction

The Company shall retain, destroy or anonymise Personal Information in accordance with all applicable laws and regulations, contractual obligations and the Company's applicable records retention and destruction policies, as deemed appropriate. Data may be retained for longer than the standard specified retention timeframes when held in connection with a query or an investigation on a matter, including suspected or actual illegal activity in which any record or other evidence of potentially illegal activity may be provided to legal authorities.

Cellmark will process and store your Personal Information only for the period necessary to achieve

the purpose of storage. If we do not need to store your personal data, or if a storage period expires, your personal data will be anonymised or erased in accordance with our company policies and legal requirements.

Standard retention timeframes

Service	Sample	Personal data
DNA Paternity/relationship testing (incl DNA at Home)	3 months	1 year
DNA relationship testing in immigration cases	3 months	1 year
Hair Drug & Alcohol testing	6 months	2 years
Blood Alcohol testing	12 months	2 years
Urine Alcohol testing	12 months	2 years
COVID-19 testing	48 hours (sample) 8 weeks (RNA/cDNA)	1 year

Retention timeframes are calculated from the date of the final test report. Timeframes may vary according to contractual arrangements. Sample/data destruction may be carried out after the timescales indicated due to operational procedures, but will be carried out within 1 month of the timescales listed. Anonymised records of testing will be retained for at least 8 years (two accreditation cycles) in accordance with UK Accreditation Service (UKAS) requirements.

XIII. Security and Storage

The Company has security programs and uses technical and organisational measures to protect Personal Information against accidental or unlawful processing and against destruction or accidental loss, destruction or damage, in particular where processing involves transmission of Personal Information over a network, and against all other unlawful forms of processing. The Company will comply with its security policies as revised and updated from time to time, together with any security procedures relevant to a business unit or function. Access to such Personal Information is limited to those who need to process it to conduct business for the Company.

The Company requires that employees and other personnel who have access to Personal Information are appropriately trained and made aware of their obligations when handling Personal Information, in accordance with the Company's policies, including this Privacy Policy. Training includes privacy training that is required of all employees at the Company and additional training that may be appropriate based on an individual's job responsibilities, business unit, and location.

Security incidents involving Personal Information shall be properly investigated and promptly remedied in the event of a breach. Any employee or other personnel handling Personal Information in connection with employees, contingent workers, study participants, investigators, or any other individual, who knowingly or recklessly discloses that Personal Information outside of the Company's policies and procedures will be subject to appropriate disciplinary procedures.

XIV. Data Incident Management and Notification

The Company will adhere to its data incident management and notification policies (as revised and updated from time to time), which set out the process that the Company must follow in the event of a security incident. As required by applicable law, the Company will:

- notify the competent supervisory authority of a data incident;
- notify Data Subjects of a data incident involving their Personal Information; and
- assess the circumstances in which such notifications may not be required.

XV. Dispute Resolution

Any questions or concerns regarding the use or disclosure of Personal Information should be directed to the Data Controller. The Company will investigate and will attempt to resolve complaints and disputes regarding the use and disclosure of Personal Information in accordance with this Privacy Policy and applicable law.

For complaints by Data Subjects relating to the collection, processing, or transfer of Personal Information for which the Company is responsible and which complaints cannot be resolved by the Company's response to the complaining party, such disputes are to be resolved in accordance with the requirements of applicable law or as agreed upon in any contract or governing documents.