

VMD Privacy Notice

This Privacy Notice sets out the standards you can expect from the Veterinary Medicines Directorate (VMD) when we collect, hold, or use your personal information and applies to any VMD website, application, product, software, or service linked to us (collectively, our “services”).

We are committed to the responsible handling and security of personal data. Your privacy is important to us and protected in law through the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Law Enforcement Directive.

Who does UK GDPR apply to

The UK GDPR applies to processing carried out by organisations operating within the UK, and to those operating outside the UK but offer goods or services to individuals in the UK.

UK GDPR applies to ‘controllers’, who determine the purpose and means of processing personal data, and ‘processors’, who are responsible for processing personal data on behalf of a controller.

As a controller, we ensure our contracts with processors comply with UK GDPR. As a processor, we have a legal obligation to maintain records of personal data, processing activities, and reporting breaches.

Our contact details

Data Protection Manager
Veterinary Medicines Directorate
Woodham Lane, New Haw, Addlestone, Surrey, KT15 3LS
postmaster@vmd.gov.uk

The VMD is an Executive Agency within the Defra group and part of Defra’s legal entity.

What is personal data

Personal data is data that identifies an individual directly or indirectly, by reference to an identifier such as their name or a unique reference number.

The type of personal information we collect

We currently collect and process:

- names and contact details
- job titles
- business names and addresses
- animal owner names and addresses
- professional organisation membership numbers and status
- medical history information if provided as part of a suspected adverse event report

How we collect your data

Most of the personal information we process is provided to us directly by you because:

- you have registered for or used our services
- you have provided it to help demonstrate regulatory compliance
- you have taken part in a survey or data collection exercise

- you have requested assistance or provided feedback
- you have reported a problem or suspected illegal activity
- you are part of a scientific or policy network

We also receive personal information indirectly, usually because:

- business associates have provided your contact details
- we gather enforcement information and intelligence from members of the public,
- the pharmaceutical and veterinary industries, and other law enforcement partners
- we receive reports of adverse events from pharmaceutical companies

Why we collect your data

We use the information given to us to:

- carry out our Public Task functions, services, or research
- help us to confirm your company affiliations when registering to use our services
- maintain records of qualified, registered, or approved businesses and personnel
- provide information that may be of interest or relevance
- seek feedback on our functions and services
- evaluate suspected adverse reactions
- investigate and monitor suspected illegal activity
- facilitate professional networks and specialist committees or groups

Under the UK GDPR, the lawful bases we rely on for processing this information are:

- Your consent. You may be able to remove your consent at any time by contacting the Data Protection Manager at postmaster@vmd.gov.uk
- We have a contractual obligation
- We have a legal obligation
- We need it to perform a public task
- We have a legitimate interest

Automated decision-making and profiling

We do not use information about you for automated decision-making (making a decision solely by automated means without any human involvement) or profiling (automated processing of personal data to evaluate certain things about an individual). We will tell you if that changes.

Who can access your personal data

Bodies charged with auditing, monitoring, or inspecting our compliance with applicable law and other standards, as necessary, and for the purposes of preventing and detecting fraud.

Staff and processors charged with undertaking activities on our behalf.

Who we share your data with

The data you provide will only be transferred to processors compliant with UK GDPR. We may share information with:

- other UK government departments and agencies
- organisations or individuals under a Data Sharing Agreement for the purposes of research

- UK, EU, and EEA law enforcement partners
- UK professional membership bodies
- UK and organisations in the EEA that we work with to deliver our services and engagement activities
- network, committee, or group members

Personal information provided as part of a suspected adverse event will not be shared with anyone outside the VMD without your express permission.

When we publish personal data

There are circumstances when we need to publish personal data and we balance the need for transparency compared to your privacy rights. As a public body we are required to be transparent about the use of money and publish Senior Executive salaries and procured contract details.

We may have to release personal data and commercial information to execute our enforcement strategy, or under the Environmental Information Regulations 2004 and the Freedom of Information Act 2000.

How we store your personal data

Your information is securely stored within systems on our premises or in cloud service centres.

We are certified to ISO27001:2022 Information Security, which means we regularly undergo rigorous audit by an accredited certification body and successfully demonstrate that we meet the requirement of the standard.

Online services and support

Data collected through our Support Service Desk is processed and stored as described with the Atlassian Privacy Policy as well this Privacy Notice.

To register to use our Veterinary Medicines Digital Service you will need to create an account with sign-in details to identify you. To ensure that you are authorised to create an account on behalf of a company we collect information on a “referee” and may contact them for confirmation.

The sign-in details you provide will be used to access several services provided by VMD to save you time. We will store basic information about you (and your business, if relevant) so that you do not have to re-enter the information each time you use our service.

Your information will be shared with the administrators associated with your account for them to manage the access to one or more of the online services you use.

To evaluate and improve our services we may store your Internet Protocol (IP) address and details about the web browser you use, and information on how you use our service through cookies and analytics.

We may contact you about our services and opportunities.

How long we store your personal data

Information that you provide, or that is provided about you, will be kept for the length of time needed to complete that function or service. Some information will be kept for the length of time that an account, registration, certification, approval, or authorisation remains in place.

Record periods are set in line with statutory, regulatory, legal, and security requirements, or for their historic value. Our retention policies are listed below. After which time we may anonymise or permanently delete it:

Function/Service	Retention policy
Surveillance schemes	7 years
Enforcement	10 years
Inspections	Life of authorisation
Complaints and enquiries	5 years
Official government correspondence	5 years
Information or access requests	5 years
Recruitment	5 years
Financial transactions	7 years
Procurements and contracts	6 years (from contract completion date)
Product related	20 years (from authorisation expiry)
Import and export	2 years
Legislation	20 years
Microchip	20 years
Incomplete or rejected online registrations	6 months
Active online service accounts	On request by you or your company
Inactive online service accounts	2 years
E-learning	5 years

Your data protection rights

If you do not wish to provide us with your information, we may not be able to provide a full service to you.

Under data protection law, you have the following rights:

- **Informed** – You have the right to be informed about the collection and use of your personal data. We provide a link to our Privacy Notice at data collection points, and we will inform you if you are affected by a breach or if processing changes, if possible.
- **Access** - You have the right request information about how your personal data is processed, and to ask us for copies of your personal information. This is called a

'subject access request' and we may ask for proof of your identity. We will respond within one month but may extend this by up to two months in complex cases. If the cost to provide you with all the data requested is excessive, we may refuse your request or ask you to provide a contribution to meet these costs.

- Rectification - You have the right to ask us to rectify personal information you think is inaccurate or to complete information you think is incomplete. When doing so, tell us where you have seen it and what you feel is inaccurate. We will respond within one month but may extend this if the request is complicated. Where we maintain that the original information held was accurate, we will explain why. If you do not agree, you have the right to complain to the ICO.
- Erasure - You have the right to ask us to erase your personal information in certain circumstances. However, we may refuse your request should the data be required to comply with a legal obligation, performance of a contract or public interest task or exercise of official authority.
- Restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- Objection to processing - You have the right to object to the processing of your personal information in certain circumstances.
- Data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.
- Automated decision-making and profiling – You have rights to ensure that decisions based solely on automated processing, which have legal or similarly significant effects, are fair and transparent. We do not use information about you for automated decision-making (making a decision solely by automated means without any human involvement) or profiling (automated processing of personal data to evaluate certain things about an individual).

A full explanation of your rights can be found on the [ICO website](#).

How to update your details, withdraw consent, or exercise your rights

If you discover that the personal data we hold about you is inaccurate, or incomplete, please tell us where you have seen it and what it should be, so we can update your records.

You can request that we

- a) no longer process your personal data and
- b) delete your personal data. However, agreement may not be assumed as we may have to refuse your request should the data be required to comply with a legal obligation, performance of a contract or public interest task or exercise of official authority. Where this is the case, we will tell you.

Contact the Data Protection Manager at postmaster@vmd.gov.uk if you wish to make any request and we will respond within 1 month. You will not be charged for exercising your rights.

Detecting and preventing fraud

The VMD has a duty to protect the public funds it administers, and to this end may use the information provided by its customers and suppliers for the prevention and detection of fraud. It may also share this information with other bodies responsible for auditing or administering public funds for these purposes.

The [National Fraud Initiative](#) is conducted using the data matching powers bestowed on the Minister for the Cabinet Office by Part 6 of the Local Audit and Accountability Act 2014 (LAAA). The Cabinet Office conducts data matching exercises to assist in the prevention and detection of fraud. The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. Our legal basis for processing your criminal convictions data is paragraphs 6 and 10.

Have any questions or issues?

If you have any questions or issues about our use of your personal information, or how we have handled your request, or to report a breach, contact our Data Protection Manager at postmaster@vmd.gov.uk

You can also contact the Defra Group Data Protection Officer, by writing to them at:

4th Floor, Seacole, Marsham Street, Westminster, London, SW1P 4DF

Or via email: DefraGroupDataProtectionOfficer@defra.gov.uk

Or the Information Commissioner's Office, the independent regulator, using their helpline number 0303 123 1113 or through ICO website <https://www.ico.org.uk>

Our [Personal information charter](#) also explains more about how we treat your personal information. If you have any questions, or would like to exercise any of your rights, please contact:

Data Protection Manager
Veterinary Medicines Directorate
Woodham Lane
New Haw
Addlestone
Surrey
KT15 3LS

postmaster@vmd.gov.uk