Veterinary PracticeToday
FOR PERSONAL & PROFESSIONAL DEVELOPMENT

Looking after data makes good business sense

Is your practice ready for the new data protection law?

SPECIAL SUPPLEMENT

GDPR checklist

- [ ] **Have you updated your privacy notice? Essential elements are:**
  - your lawful basis or bases for processing data. If using legitimate interests, you must state what these are
  - your purposes for processing data
  - who you share data with
  - what your data retention policy is
  - the rights individuals have with regards to their data, including the right to be forgotten
  - the details of any automated decision making when processing their data
  - the right for clients to object to their data being processed based on legitimate interests and also to direct marketing.
- [ ] **Have you updated your internal documentation? Essential elements are:**
  - which lawful basis you are relying on for each specific processing activity and the justification for each. These should be 'necessary for the contract' and 'legitimate interests' for the majority of cases
  - which specific processing activities you are doing and the purposes of these
  - any third parties that process information on your behalf and any joint controllers
  - the categories of individuals you hold data for (employees, clients), the categories of the data (financial, contact details, animal health data) and the categories of any recipients of the personal data you collect
  - any third countries and organisations that you share data with and the safeguards in place for these data transfers
  - retention schedules for different categories of personal data
  - a description of your safeguards (technical and organisational) in place for protecting personal data.
- [ ] **Have you carried out an information audit to establish the specifics of personal data handling within your business – who is the controller, who are the processors, what processing is being done, is it necessary? Do you have a contract in place with all processors that you use?**
- [ ] **Are you ready to provide clients with privacy information at the time you collect the data?**
- [ ] **Have you communicated your privacy information to clients?**
- [ ] **If relying on legitimate interests as a lawful basis, have you performed a Legitimate Interests Assessment?**
- [ ] **Do you have a response plan for dealing with data breaches?**
- [ ] **Do you have breach detection methods in place?**
- [ ] **Are staff aware of who will conduct any data breach investigations and report to the relevant authorities?**
- [ ] **Have you reviewed your retention policy, outlining your retention period and how data will be removed?**
- [ ] **Do you have a procedure in place for data requests and are staff aware?**
- [ ] **Have you conducted and documented staff training on data protection, focusing on the following areas:**
  - use of personal mobile devices & smartphones within the practice
  - password protection and secure logins to practice IT systems
  - dealing with information requests
  - who should be informed if a suspected data breach occurs
  - use of USB storage devices and unencrypted laptops
  - storage of personal data both digitally and in paper format.

Disclaimer: Every practice should make its own decisions about how to comply with its legal requirements. This article is not intended to provide legal advice.

Andrew Horrex
BSc(Hons)

Andrew graduated from Brunel University with an Honours degree in Computer Science in 1992. He started his IT career as a software developer and has had various roles in the IT industry over the years, including IT Manager, Development Manager, Senior Software Developer and Software Architect. He has 30 years' experience in the IT industry and has worked at AT Veterinary Systems for over 15 years.

**Suggested Personal & Professional Development (PPD)*

COMMUNITY REVIEWED™

GDPR

Looking after your clients' data: All you need to know

Veterinary practices have many professional responsibilities, most of which are specific to the veterinary work that they perform. However, they also have the responsibilities associated with every business entity. Looking after client and staff personal information, ensuring it is kept safe and not used in any way that they do not wish, is best practice and something that should be embraced and promoted.

Upcoming legislation – the General Data Protection Regulation (GDPR) – will make this a legal requirement from 25 May 2018 and this article explores the implications of this, as well as new privacy regulations.

Veterinary practices need to look at and update their current terms and conditions and data protection policies, to ensure they comply with the regulations. It is also important to appreciate the benefits of improving the way you handle personal data within and outside of the practice.

The primary aim of the GDPR is to establish a standardised data protection framework, enabling data to flow freely and securely, and to simplify the regulatory environment for international businesses by unifying the regulation within the EU. The rapid development of technology has allowed both public and private companies to make use of personal data, but with this has come the dramatic increase in security breaches, putting the personal data of millions of citizens at serious risk. Yahoo, eBay, TalkTalk, Ashley Madison and Carphone Warehouse are just a few of the large companies that have been affected. The new regulations are designed to minimise these potential and real risks.

The GDPR differs from the Data Protection Directive (DPD), which only set out objectives for member states to achieve, rather than laws to abide by. So whereas now there are no hard and fast rules for handling data between different EU countries, when the regulation comes into place all businesses who wish to trade data within and with the EU must comply. It is because of this that – despite Brexit – it is still important for UK businesses to have a good understanding of the regulations and how they apply to them. Post-Brexit, those businesses trading in the EU will still need to demonstrate compliance with the GDPR. Regardless of the Brexit issue, businesses in the UK must prepare for the GDPR as a new Data Protection Bill was published in September 2017. The new bill contains the majority of the provisions of the GDPR.

The regulation applies to any organisation that collects

GDPR key changes

- organisations must notify any data breaches within 72 hours
- individuals will now need to actively give consent for their personal data to be processed – implied consent is no longer acceptable
- individuals will have the right to retract consent and request data erasure (the right to be forgotten). They will also have a 'right to data portability'; allowing them to request data in a readable format
- there will be a two-tier fine policy and failure to comply to the new rules will attract the following fines:

Tier 1 serious breaches: fine of up to 20 million Euros or 4 per cent of global turnover, dependent on which is greater.
Tier 2 lesser breaches: fine of up to 10 million Euros or 2 per cent of global turnover, dependant on which is greater.

What counts as a 'legitimate interest'?

Most veterinary activities where the data subject is a client of the practice will imply a legitimate interest. A client has to reasonably expect at the time and in the context of collection of personal data that processing for that purpose may take place.

Regarding direct marketing, the GDPR states that 'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. (4)' ICO guidelines explain that if you can show proportionate use, minimal privacy impact and that clients would not be surprised or likely to object, legitimate interests can be relied upon as a lawful basis for marketing activities. Remember that the right to object requires processing to stop immediately for that client.

data from EU residents. Your veterinary practice falls into this category and, under the new regulations, will be considered the registered data controller (see later for definition). There is a two-tier system of very hefty fines for organisations that do not comply with the regulations after May 2018. Any practices that have not yet started to assess their compliance would be wise to do so as soon as possible.

The GDPR will focus on data protection from the initial identification and protection of personal identifiable information (PII), through to the required prompt notification of a data breach incident to the relevant supervisory authority.

GDPR compliance will add new security responsibilities and obligations once it comes into force and, put very simply, you will have to:

- make sure you know the type of data your business processes, how and where it is used, keep a record of data operations and activities and consider if you have the required data processing agreements in place
- update your T&Cs to inform clients of data processing activities
- carry out privacy impact assessments (PIAs) on products and systems and ensure they adequately protect the data they hold
- review processes for the collection of personal data
- implement 'privacy by design' and 'privacy by default' in your practice and assess whether existing products meet GPDR standards
- be aware of your duty to notify the relevant supervisory authority of a data breach.

Before looking in more detail at the steps you need to take, it will be useful to become familiar with the key terms associated with the new regulations:

Key terms

Personal data

Any information that identifies a living individual (this only applies to humans). Any information which, if put together with other information, would identify a living individual.

Sensitive information

Any information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

Individual rights

The individuals whose data is kept in your system are given certain rights by the GDPR concerning the data and its use:

1. **The right to be informed** about how the data is used. This means you must have a system that can provide 'fair processing information' and ensure transparency on how you use personal data
2. **The right of access** – the right of individuals to have access to the personal data you hold. Data controllers must respond within one month to any application for access to data and are not able to charge for its provision
3. **The right to rectification** – individuals have the right to have personal data rectified if it is inaccurate or incomplete
4. **The right to erase** – also known as 'the right to be forgotten'. This is the right of the individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing
5. **The right to restrict processing** – the right of the individual to 'block' or suppress the processing of personal data, for example if there is some kind of dispute. While processing is restricted, you can retain just enough information about the individual to ensure that the restriction is respected in future
6. **The right to data portability** – this allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data from one IT environment to another in a safe and secure way, without hindrance to usability
7. **The right to object** – individuals have the right to object to processing, based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing and processing for purposes of scientific/historical research and statistics
8. **Rights in relation to automated decision making and profiling** – this safeguards individuals against the risk that a potentially damaging decision is taken without human intervention. Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

 Disclaimer: Every practice should make its own decisions about how to comply with its legal requirements. This article is not intended to provide legal advice.

Data subjects
The individuals whose data is stored.

Data controller
The person or organisation that determines the purposes for which, and the manner in which, any personal data are, or are to be processed. All legal responsibility for compliance to the new regulations falls to the data controller. This means that when a data controller discloses personal data they must already have a written contract in place saying what the processor may or may not do with any released data. The data controller also has a duty to ensure that the data processor's security arrangements are at least equivalent to their own and take reasonable steps to ensure that security is maintained. For the purposes of this article, the data controller would be the veterinary practice.

Data processor
The person or organisation which processes personal data on behalf of the controller. This could be an external company that the practice uses for mailings, for example.

Processing
Everything which is done with the data obtained, including organisation, adaptation or alteration of the information or data, retrieval, consultation or use of the information or data, disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.

Data breaches
A data breach would be considered to be loss, damage or destruction of personal data and unauthorised disclosure, access to, or alteration of personal data. All appropriate staff need to know how to spot a data breach. Individuals must be informed of a data breach if it is likely to result in a high risk to their rights and freedoms.

A breach notification must contain:
- the nature of the personal breach, including the numbers of individuals and personal data records concerned
- the name and contact details of the data protection officer, or other contact point where information can be obtained
- a description of the likely consequences of the personal data breaches
- a description of the measures taken to deal with the breach
- a notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organisation discovering it.

The GDPR defines a number of key data protection principles for organisations.

Lawful basis for processing
Under EU data protection law, there must be a lawful basis for all processing of personal data. Personal data may be processed only if at least one lawful basis applies. There are six available lawful bases, listed below.

1. **Consent** – an individual has given consent for processing
2. **Contract** – processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a new contract
3. **Legal obligation** – processing is necessary for complying with the law
4. **Vital interests** – processing is necessary to protect someone's life
5. **Public task** – processing is necessary for you to perform a task in the public interest and the task has a clear basis in law
6. **Legitimate interests** – the processing is necessary for your legitimate interests, unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

It is down to the practice to decide which is the applicable basis for each processing activity (see next section to find out what constitutes processing), and to communicate this to clients. This means informing clients before 25 May 2018 and updating your privacy policy. Once a lawful basis is determined, it should not be changed unless your purposes change. If consent is your chosen basis, you will need to seek fresh consent for any new purposes.

"Complying with the new regulations can be separated into three stages - identification, planning and actions"

Personal data must be:
- processed fairly, lawfully and with transparency
- collected for specific, explicit and legitimate reasons
- adequate, relevant and necessary for the purpose it was collected
- accurate and up-to-date
- kept in an identifiable form no longer than is necessary – if data is to be kept, it should be anonymised where possible
- processed securely – IT secure (e.g. with the use of firewalls and passwords), physically secure (e.g. use of lockable filing cabinets), organisationally secure (e.g. adhering to practice policies and training).

So what do you need to do?

Complying with the new regulations can be separated into three stages:

1. Identification
2. Planning
3. Action

1. Identification

You need to identify within your organisation:
- what personal data includes, for both staff and client data. This will encompass staff data such as CVs, job application forms, sick notes, health records, disciplinary procedures, salary information, holiday requests, bank details, etc. Client details can include name, address, telephone number, financial information etc. Pet details are not regarded as personal data in the regulations, unless they can be used to identify owners – an unusual pet's name for example
- how personal data is stored – the data you hold will be in a number of formats; paper, emails, hard drives, USB drives and IT management systems
- what data is held and transferred – the data you have may be held by individuals, practices or groups of practices, by departments within a practice, or by individuals within departments. The important thing is that you know who holds/has access to data. The data may be transferred interdepartmentally via electronic devices, by email or in paper format, as well as actually being sent to outside bodies – for example to laboratories on forms, or in the cloud
- what data is transported from the building – in some instances, data may be physically transported to other sites, into the field (in the case of large animal vets on visits), or to an individual's home. The data may be in electronic or paper format
- identify potential weaknesses to data security – DMZ, firewall, virus and trojan protection systems.

2. Planning

Having gathered information on all types and formats of data held, the second stage is to formulate a plan of action that will ensure compliance with the new regulations.

Do consider:
- how data is requested
- the lawful basis for processing client data
- how you will ensure that a lawful basis is in place for the different processing activities that you might put an individual's data through
- what will personal data be used for? For example, you may just use it as a contact record, you may wish to use an email to remind a client of an appointment, you may wish to send them product or service details, or you may wish to send their details to a third party
- identify all phones, laptops, tablets and any other devices that hold personal data
- what are the individual responsibilities of your staff, with regard to personal data held?
- what policies need to be written to ensure compliance?
- what changes to your terms and conditions or privacy notice are required for transparency?
- what training will employees need, to ensure that the whole practice understands and complies with the new regulations?
- identify the data processors that the practice works with; this will include organisations such as laboratories, insurance companies, debt collectors and any company involved in holding data or disposing of data
- how will you deal with data breaches?

3. Action

You now need to put your plan into action.

Personal data

Personal data should be processed lawfully, fairly and in a transparent manner in relation to individuals.

After 25 May 2018, practices will need to have a lawful basis for processing personal data. One lawful basis for processing data, is when processing is necessary for the performance of a contract with the data subject.

"Any changes in the use of data will attract the need for new consent"

 Disclaimer: Every practice should make its own decisions about how to comply with its legal requirements. This article is not intended to provide legal advice.

Veterinary practices may use this lawful contract basis for the majority of daily tasks, where the contract is that of animal health care. This is implied, but should also be displayed on your terms and conditions and privacy notice. To comply with transparency, practices should have a clear privacy notice on their websites and reception, explaining in plain language how personal data will be used for the care of their animals. Clients should be informed of the intended processing purposes and the lawful basis before 25 May 2018.

Processing insurance claims also falls under the performance of the contract.

Microchip registration of dogs is necessary for compliance with a legal obligation, so has a lawful basis, but microchip registration of cats, exotic pets and horses may need special mention under reunification services.

Additionally, any processing that is necessary for the purposes of legitimate interests pursued by a practice are lawful, except where these interests are overridden by the interests, rights or freedoms of clients.

These legitimate interests should be stated on the practice privacy notice. Legitimate interests is the most flexible lawful basis for processing. It does however require that the processing is necessary. If the result can be achieved in a less obtrusive way, then legitimate interests do not apply.

The data that is collected from clients should only be used for the original purpose stated in the privacy policy and for which a lawful basis is valid. Further processing is not permitted without another lawful basis. A veterinary practice, for instance, may consider that further processing of personal data is justified for statistical purposes, archiving in the public interest or scientific research.

Only client data with a valid lawful basis should be collected and stored.

Practices should maintain up-to-date records and remove inaccurate data. It is good practice to regularly seek updated client information.

Veterinary practices could be considered to have a clear mandate for storing (a form of processing) client data for historical clinical analysis and referral information.

Practices should implement secure IT systems and deliver relevant organisational change, focussing on data security and privacy.

Consent

Where there is no other lawful basis for processing data, consent of the client will need to be obtained.

Consent is not appropriate if you would still process the data on a different lawful basis, if consent is asked for as a precondition of service, or if you are in a position of power over the individual.

Any consent must have been fully explained, regarding what will be done with the data. Any changes in the use of the data will attract the need for new consent. Consent must also be obtained from those sending unsolicited data, if that data is to be kept or used by the business – e.g. unsolicited CVs or job enquiries. This means that all consent requests, be they paper-based or digital, will need to be designed in such a way as to comply with these regulations, with the concept of privacy by design constantly in mind.

Direct marketing is the most likely area where consent is required in a veterinary practice, although legitimate interests can be relied upon. There are already provisions in the Privacy and Electronic Communications Regulations 2003 regarding marketing calls and messages. Current ePrivacy legislation allows opt-out and pre-filled opt-in for marketing. However the policy is expected to be updated later this year, with higher protection safeguards against unwanted marketing. One of these safeguards will likely be (based on draft legislation) a positive opt-in requirement for direct marketing. It makes sense for veterinary practices to account for this in their GDPR planning.

Asking for consent

- check that consent is the most appropriate lawful basis for processing
- make the request for consent prominent and separate from your terms and conditions
- ask people to positively opt in
- don't use pre-ticked boxes or any other type of consent by default
- use clear plain language that is easy to understand
- specify why you want the data and what you are going to do with it
- tell individuals they can withdraw their consent
- ensure that individuals can refuse to consent without detriment
- don't make consent a precondition of a service.

vetcommunity.com

The website for veterinary professionals

My Profile • My PPD Log • Blogs • Abstracts • Articles • News • and More

If a practice deems consent necessary, the considerations listed previously could be incorporated into a separate consent form as evidence. This could be a digital form and doesn't explicitly require a signature. Answering 'yes' to a clear oral consent request is an acceptable 'opt-in' mechanism. This means staff can ask about the specific areas of data processing and fill in digital forms for the client. Obtaining consent in this way provides an easy method for recording crucial information (timestamp, employee login, consent request phrase) and allows version updating and consent withdrawal. The form should keep a record of exactly what was said at the time. A response to an email with an express statement confirming consent is also a positive opt-in mechanism.

It should be made obvious to clients how to withdraw consent – this should be incorporated in the consent request form and also in your privacy policy. A privacy policy notice on reception is a good idea.

There is no need to seek fresh consent if you have it already and it is in line with the GDPR standards. For many veterinary practices, this is not the case and new consent should be requested for direct marketing unrelated to animal health.

Recording consent

- keep a record of when and how you got consent from the individual
- keep a record of exactly what they were told at the time
- keep a record of who obtained the consent.

Managing consent

- regularly review consents to check that the relationship, the processing and the purposes have not changed
- have processes in place to refresh consent at appropriate intervals
- make it easy for individuals to withdraw their consent at any time and publicise how to do so
- don't penalise individuals who wish to withdraw consent.

Individual rights

For veterinary practices, this gives a necessity for clear communication of how client data will be used, how it can be edited or erased and how to ask for data processing activities to be stopped. Additionally, clients should be informed of how they can access their personal data. This can be achieved by a copy of your privacy notice on reception and on your website. A privacy notice could be given to new clients at registration.

Some direct messaging tools are at risk of restricting the right related to automated messaging. Tools that give a human intervention before sending should be implemented in this instance.

Where clients have requested their data, practices should provide it within one month. A note should be added if information will be stored in the client card that is not personal information or supplementary information.

Paperwork

All paperwork and files must be locked away when not being used. This applies to both office and home use of any paper documents which contain personal data.

Electronic data

All computer files – including emails, back ups and memory sticks – containing personal data must be password protected, with access being limited to 'need to know' individuals. This applies to home and office use.

Clear desks

A clear desk policy could be implemented, so that at the end of each working day no personal data is left on desks.

What needs to be recorded on your internal documentation?

The Information Commissioner's Office (ICO) recommends the following:

- name and details of your practice and your Data Protection Officer (DPO)
- purposes of processing client data
- description of the categories of individuals and of personal data collected
- categories of recipients of personal data (your third party processors)
- details of transfers to third countries, if any, and the transfer safeguards in place
- retention schedules
- description of technical and organisation security measures.

The ICO also provides documentation templates for controllers and processors at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation

Training
All employees should receive training on the basic requirements of the GDPR. For those identified employees, there should be training on the specifics of secure data storage within the organisation. Staff should also receive training regarding the transporting of data between sites or from site to home.

Data transference
All data sent to a third party should be pseudonymised where possible.

Old data
Data that is no longer required (perhaps because the client has left or their pet has died) no longer needs to be retained legally by the practice and should be destroyed in a safe and secure manner. The practice should have a policy on how long personal data will be kept and how it will be destroyed.

Archived data
Any archived data, i.e. data that is not in active use, but needs to be retained for business or legal reasons, should be encrypted.

Removal of data
An individual may request the removal of their personal data from your system. You must comply with this if the data cannot be shown to be needed by the business for legal reasons, e.g. retention for tax, VAT requirements. So it would be wise to include in any data protection policy the method by which agreement or refusal to such a request would be determined.

Provision of personal data on request
Individuals can request copies in a readable format of their personal details but this does not include those of their animals under GDPR. The practice must ensure that all staff are aware of this, who to consult for approval and how to provide the requested data.

Devices holding personal data
Having identified all the devices that hold or could potentially hold personal data, ensure that they are all password protected and encrypted if they leave the premises.

Your data processors
The data processor handles data on behalf of your practice e.g. laboratories, payroll, shredding companies, those handling email reminders and cloud providers, IT providers, etc. You must have a legal contract with these processing companies that is GDPR compliant and sets out your role as the controller and what you authorise the processor to do with the data they are sent. Note that any data breach by the processor will be the responsibility of the data controller, if the controller does not have a contract in place.

"Processing data must be done in a manner that ensures its security. Anonymisation and pseudonymisation should be used wherever possible."

Appoint a person responsible for implementing data security. Although this may not be a legal requirement for your organisation, it would be good practice to do this.

GDPR statement or privacy policy
The practice data protection policy should be updated to include reference and adherence to the GDPR. This requires information to be provided to the client at the time the data is collected.

Some of the required information is listed below:
- identity and contact details of the controller. In most cases, the controller is the veterinary practice
- the contact details of the Data Protection Officer (DPO). You may not have to appoint a DPO but it is good practice to appoint a person responsible for data protection within the practice
- the purposes of the processing for which the personal data are intended and the legal basis for doing so. The purpose could be defined as the provision of animal care (both emergency and preventative) and the legal basis may be for this contractual fulfilment
- the legitimate interests pursued by the controller or third party. These could include preventative health care and practice updates and news. Processing insurance claims, sending tests to laboratories and messaging services should be mentioned here if your practice provides these
- the recipients of personal data, if any. If a practice passes on client information to third parties, they should be mentioned here

 Disclaimer: Every practice should make its own decisions about how to comply with its legal requirements. This article is not intended to provide legal advice.

- that the controller intends to transfer data to a country outside the EU or international organisation, if applicable. This raises the question of third parties where data is stored outside the EU. To minimise the risk of not having these organisations cited on your GDPR form, staff should be trained where they can and cannot send client data. Please note that the use of personal mobile phones and some applications presents potentially high risks of data breaches
- the period for which personal data will be stored
- the rights outlined above and the right to withdraw consent
- the right to lodge a complaint with a supervisory authority
- whether the provision of personal data is a contractual requirement and if the client is obliged to provide their personal data. The possible consequences of failing to provide personal data should also be included
- the existence of automated decision-making, meaningful information about the logic involved and the significances and consequences of this form of processing. Practices should aim to reduce forms of decision making with no human interaction
- where further processing will be done, the practice should give details of these. Historical clinical analysis and statistical analysis could be mentioned, together with any relevant information on these forms of processing.

These points can be incorporated into your terms and conditions or added as a separate GDPR statement.

Accountability and governance

The Information Commissioner's Office (ICO) has provided a number of measures that promote good accountability and governance regarding data protection.

These are outlined below:

- you are responsible for and must be able to demonstrate that you are in compliance with the GDPR principles. You must put into place comprehensive but proportionate measures to minimise the risk of data breach. These may include internal policies, staff training, internal audits of processing activities and reviews of HR policies and secure network controls
- written contracts between controllers and processors should be in place. These should contain terms that show adherence to the GDPR requirements. Practices are liable for their compliance with the GDPR and should only use processors who provide sufficient guarantees that the requirements will be met. Processors must only act on the documented instructions of the practice and must not engage with another processor without authorisation from the practice. Processors also need contracts in place with other processors. See the ICO draft guidance on contracts and liabilities for details of what should be included in your contracts
- relevant documentation on processing activities should be maintained. If your organisation has less than 250 employees you are required to maintain records of higher-risk processing activities and non-occasional processing activities. If your organisation has more than 250 employees you must maintain additional internal records of all processing activities
- data protection and privacy by design guidance should be followed to protect the rights of data subjects. Measures such as pseudonymisation, data minimisation, restriction of access to client data and Privacy Impact Assessments (PIA) should be implemented, particularly when using data for new purposes or strategies
- data PIAs should be performed whenever implementing a new service or where processing data results in a high risk to the rights and freedoms of individuals
- veterinary practices are not obliged to appoint a DPO, unless they carry out large scale processing of special categories of data, or carry out large scale monitoring of individuals. This does not mean that appointing a DPO is a bad idea, as practices still have an obligation to ensure staff have the skills to meet GDPR obligations. A DPO could be tasked with delivering best practice training to staff and monitoring compliance.

"The onus is upon every veterinary practice to identify the personal data within their organisation, devise a plan of action for GDPR compliance and then put that plan into action before 25 May 2018"

Security

Processing (which includes storing) data must be done in a manner that ensures its security. Protection against unauthorised/unlawful processing, accidental loss, damage or destruction must be provided. The ICO has well established guidance on privacy and electronic communications.

Here we discuss some key areas and pose some questions for veterinary practices:

- anonymisation and pseudonymisation should be used wherever possible. This is particularly important when transferring data outside of your practice. Laboratory tests, diagnostic analysis, telemedicine, accountancy and marketing services are areas where you should consider if personal data should be sent to a third party. If necessary, can the data be anonymised? Your IT provider should provide a unique identifier for these purposes
- does your IT partner provide an audit service for your practice? These can help assess threats and identify security risks before a data breach occurs
- do you use online registration and appointment booking services? If so, can you verify that they are GDPR compliant and are storing data within the EU?
- what security measures does your practice network have in place? Practices should regularly review their internet

security, as this is the most likely cause of a data breach. What firewalls and gateway configuration do you have to restrict internet access?
- are staff allowed to download files and install applications on the practice network?
- is your wi-fi configured with appropriate passwords (not the router defaults)? All of these should be reviewed and relevant restrictions put in place.

Does your practice have a mobile phone policy and acceptable use policies for electronic communications? Your practice terminals should have suitable safeguards in place. These include complex alphanumeric passwords, individual logins, removal of unused and outdated software and adequate erasure of data when disposing of equipment. Mobile devices should be encrypted and have a short auto logout time.

Access control to practice data is paramount for protecting your business and its reputation. Your IT solution provider should provide specific logins for each member of staff and privilege levels for appropriate access to certain areas of the system. Centralised storage of data means that data is not on the device in the first place and so no loss occurs in the event of hardware theft. Server rooms should be kept under additional protection and backup devices should not be left unattended.

Bring your own device to work (BYODW) should be discouraged in favour of locked down secure terminals.

For staff accessing the practice network from home or via the cloud, consideration must be given to where the data is stored. Who is the remote computing facility provider? Are you happy that they meet the GDPR requirements? Do you have a contract in place? What client data do they have access to?

Large data breaches in the NHS due to malware made headlines in 2017. Appropriate anti-malware and anti-virus products should be installed but not relied upon exclusively. Keep them up-to-date and take suitable action if malicious files are detected. Having a regular off-site backup strategy will help in the event that your practice data is compromised by 'ransomware'. It is also essential for 'the ability to restore the availability and access to personal data' – a requirement of the GDPR.

Training staff to be vigilant against cyber-security threats is paramount. Awareness of phishing emails, security software warnings and the risks of posting practice information to social networks should be taught.

International transfers

Additional restrictions are in place when transferring data outside of the EU or to international organisations. These ensure the same level of protection is provided in these cases.

Data transfers outside the EU are allowed when adequate safeguards can be provided. If the data transfer is necessary for the performance of a contract, or consent has been given by the client, data transfer is not prohibited.

Data breaches

Notifiable data breaches must be reported to the relevant authority within 72 hours of awareness of the event. Failure to report in this timeframe can result in significant fines (up to 10 million Euros or two per cent of global turnover).

Information on breaches can be provided in stages, as your investigation continues. A personal data breach entails any security breach that leads to the destruction, loss, alteration, unauthorised disclosure of or access to personal data. ■

Bibliography

European Parliament, Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 5.

Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 6.

Directive (EU) 2016/680. European Parliament, Council of the European Union. April 2016, Official Journal of the European Union.

European Parliament, Council of the European Union. REGULATION (EU) 2016/679 Article 47, Official Journal of the European Union. April 2016.

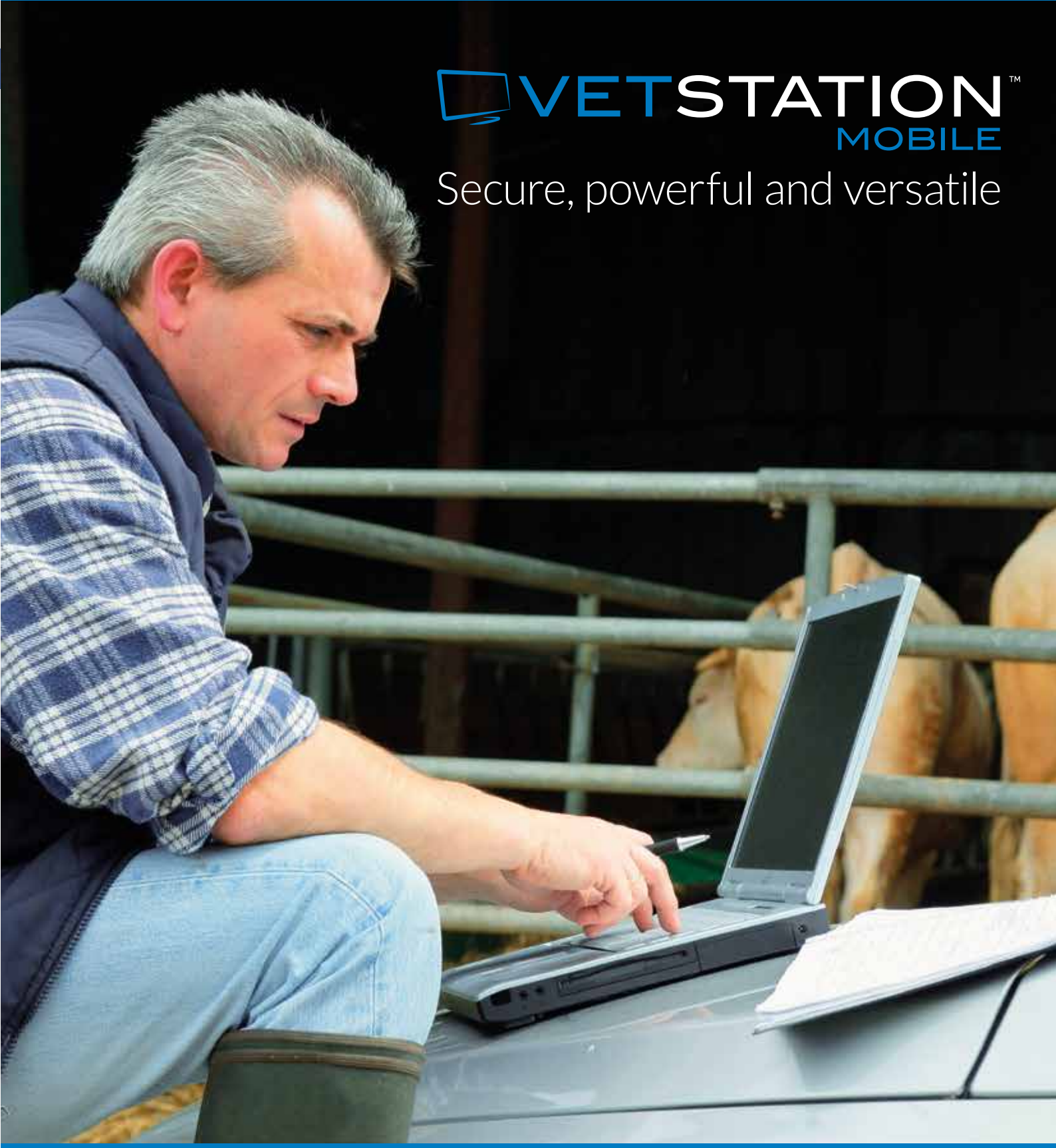
Regulation (EU) 2016/679 of the European Parliament, Article 14.

Information Commissioner's Office. Guide to the general data protection regulation. [Online] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

Data protection and privacy and electronic communications guidance index. [Online] https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/.

European Parliament, Council of the European Union. Regulation (EU) 2016/679 of the European Parliament, Article 32.

 Disclaimer: Every practice should make its own decisions about how to comply with its legal requirements. This article is not intended to provide legal advice.



The most powerful computer for equine and large animal vets

To find out more about VetStation Mobile
tel: **01359 243 400** *or* email: **enquiries@vetsystems.com**

AT VETERINARY SYSTEMS
www.vetsystems.com

Supporting you with GDPR compliance

AT Veterinary Systems is a market leader in data security and privacy by design principles in the veterinary industry. The Spectrum IT platform is inherently secure and has innate privacy features.

This section details some of the robust, GDPR-compliant features available from AT Veterinary Systems:

1. Client Contact Preferences provide specific and granular consent in line with the GDPR. Each client can have preferred contact details set for different communication types, ranging from reminders and attendance checking to product recalls and marketing. The Spectrum DDS reminder feature allows consent to be tracked with a timestamp, user, issue date and expiry date to meet the above-mentioned requirements. Additionally, a 'no mailing' flag provides a final restriction to all client communication.

2. Access control features such as individual user privileges, auto logout and Mobile VetStation encryption are key for client data protection. User privileges can be time specific, which further helps restrict access to when needed.

3. AT utilises Mac OSX and UNIX-based systems for their reliability and resilience against viruses and trojans.

4. With network protection playing a large role in a practice's defence against data breaches, AT pioneered the V-BOX. This IP device grants network access to only trusted locations outside the practice. It also creates a DMZ, an area for holding and restricting unwanted network traffic.

5. A premium network service available to AT customers is Vision Sentinel Security. This creates unique device fingerprints for all networked terminals and will reject any intrusions from non-fingerprinted devices.

6. Terminals within a practice present a large risk to your client's data, with staff often unaware of the potential for breaches through their improper use. AT has long championed the use of secure workstations and developed the VetStation for protected use. The VetStation series provides all the functionality essential for practice tasks, but with a fraction of the security risks of a PC. Virus and Trojan infections are greatly reduced with a VetStation and AT terminals possess the added benefit of having minimal client data residing on the device.

7. Spectrum DDS maintains full audit trails of client data, an essential feature for monitoring data processing.

8. Every client and patient receives a unique reference code in Spectrum DDS, which can be used to anonymise any data leaving the practice.

9. Spectrum's Laboratory Information Management System (LIMS) includes an additional pseudonymisation feature and a configuration option to omit client details from printed lab request forms. The Work Request ID is a secondary anonymised identifier that can be passed externally, used for linking lab results to specific requests and the patient record.

10 AT's cloud services are managed and delivered by AT and no third parties. Our secure data centres are based in the EU, as are our backup storage facilities, meaning additional restrictions regarding transfers outside the EU are not applicable.

11 AT's security audit (a PIA) provides practices with an analysis of potential threats to the practice IT.

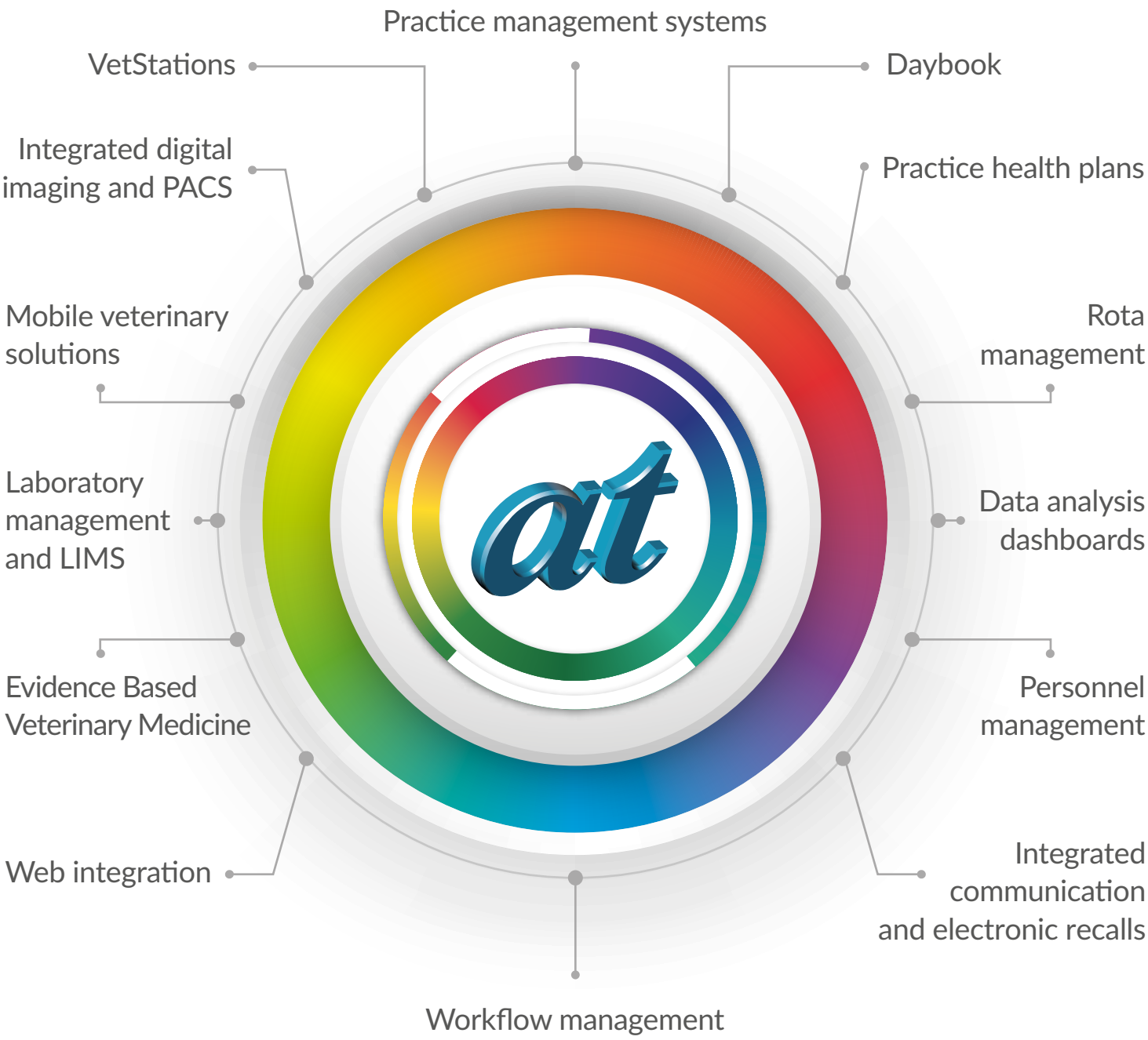
12 Human intervention is required for client communication activities.

For more information about VetStation Mobile or to find the complete practice solution fitted to your needs, contact AT Veterinary Systems today.

Phone: **01359 243 400** · Email: **enquiries@vetsystems.com**

AT VETERINARY SYSTEMS
www.vetsystems.com

Integrated technology solutions
for the modern veterinary practice



AT VETERINARY SYSTEMS

To find out more tel: **01359 243 400** *or*
email: **enquiries@vetsystems.com**

www.vetsystems.com