General Data Protection Regulations

RCVS information and Q&As

March 2018

RCVS SETTING VETERINARY STANDARDS

Introduction

1. The General Data Protection Regulations (GDPR), will be implemented in the UK on 25 May 2018 and will replace existing data protection legislation, the Data Protection Act 1998 (DPA).

2. The GDPR is important because it increases the regulatory burden and obligations on organisations and strengthens the rights of individuals.

3. The potential fines for a data protection breach have also been increased substantially. Non-compliance with the GDPR could lead to sizeable financial penalties amounting to a small percentage of annual turnover for the most serious infringements such as insufficient consent to process data. GDPR sanctions are appealable.

4. The Information Commissioner's Office (ICO) is not trying to put organisations out of business, but highlighting how important compliance with the GDPR is. The ICO will usually work with organisations to achieve compliance. It issues fines only in the most serious cases.

5. This information and Q&As are provided for general information only. They are a brief summary of the law as we understand it at the date of publication. You should obtain legal advice or consult the ICO if you are uncertain about any aspect, or if you need more detail. More guidance will be issued by the ICO in the coming months, and more legislation will be implemented, so you should check the ICO website for updates.

6. This guidance note contains links to other websites not owned or operated by us. We are not responsible for the information contained on those websites.

Key information

Terminology

7. The GDPR applies to **personal data**. These are data from which you can identify a living individual. The GDPR does not apply to data from which you can identify an animal. Examples may include: Human Resources (HR) records, customer lists, contact details, CCTV recordings and computer records. Opinion, for example, about an individual employee's performance, if held as data, can also amount to personal data (potentially of the person who stated the opinion, as well as the employee's), as can online identifiers such as IP addresses.

8. The GDPR also covers a further category of data, called 'special category' or **sensitive personal data**, which receives greater protection. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/. This category includes data about an individual's race, ethnicity ,religious beliefs, health, trade union membership, sex life or sexual orientation and now also includes genetic data such as DNA. The processing of data relating to criminal convictions is also restricted and further information can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

9. Data processing is everything you do with personal or sensitive personal data from the moment you obtain it to the moment you destroy it.

10. Personal or sensitive personal data that has been processed will relate to a data subject (an individual) such as a staff member or client of the practice.

11. In processing data, the GDPR therefore affects the following people:

    a. **data controllers** such as a practice partner or director who says what data is processed and why; and,
    b. **data processors** such as a contractor, eg a laboratory that receives samples incorporating personal data, or text and email reminder services, who therefore processes data on the controller's behalf.

12. **Consent** must be freely given, specific, informed and unambiguous, and it must be given by some affirmative action, ie an 'opt in'. Pre-completed tick boxes and 'opt outs' will no longer be effective. Consent needs to be requested in plain language and to be capable of being withdrawn at any time. Separate consent should be obtained for each proposed use of personal data. Records must be kept of the consents that have been obtained.

13. **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

Principles of GDPR

14. The principles of the GDPR are:

    a. Data must be processed **lawfully, fairly and in a transparent manner.**

    b. Data must be collected for a specified, explicit and legitimate purpose (**purpose limitation**). You need to think about why you need the data and what you are going to do with it.

    c. Data processed must be adequate, relevant and limited to what is necessary (**data minimisation**).

    d. Data processed must be **accurate** and, where necessary, kept up to date.

    e. Reasonable steps must be taken to rectify data that is inaccurate. Check that your systems are in place to make sure you keep data up to date.

    f. Data must not be kept for longer than is necessary (**storage limitation**). Have you thought about how long you need to keep different types of data and how and when do you destroy it? Data must also be kept in a form which permits identification of the data subject for no longer than is necessary for the purpose for which the personal data is processed.

    g. Organisations must take appropriate technical and organisational measures against

unauthorised/unlawful processing, loss, damage or destruction (**integrity and confidentiality**).

15. To process **data lawfully**, practices will have to satisfy one of the following conditions that relate to how that data is held: (**NB** there are additional requirements for **special category data (paragraph 8)** – primarily, obtaining explicit consent.)

    a. You must have the **consent** of the data subject, eg client;

    b. Processing the data must be necessary for performance of a **contract** or necessary in order to enter into a contract;

    c. The processing is necessary for compliance with a **legal obligation**, eg tax/pensions records, controlled drugs records; and,

    d. Processing is necessary for the purposes of **legitimate interests**, eg a business interest such as updating a client's contact details or engaging a debt collection agency to seek repayment of a debt, except where such interest is overridden by the interests, rights or freedoms of the data subject.

16. In dealing with day-to-day clients, a., b. and c. are likely to be the most common basis for processing personal data.

17. If you are relying on condition b. above (necessary for the performance of a contract), and a client moves to another practice, you would have to rely on another basis to process the data, eg compliance with a legal obligation such as retaining to satisfy regulations, or legitimate interests, such as the defence of potential claims, legal proceedings, fee disputes etc.

18. Data needs to be processed **fairly**, which includes a balance of fairness to the data subject and the data controller.

19. There needs to be **transparency**, which is about providing information to the data subject that is concise, easily accessible and easy to understand. This is commonly done through a privacy policy (see paragraph 19).

20. One of the key requirements of the GDPR is increased **accountability**. Practices will now be expected to show how they are compliant with the GDPR through their internal policies and procedures. Practices will also be required to show how such policies have been implemented and that they use data protection impact assessments where appropriate. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

21. The GDPR also requires practices to have detailed **privacy notices** explaining how they process data, which are concise, transparent, clear and easily accessible. Further information on this can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

What rights do people have to information held about them?

22. Data subjects have the **right to be informed** and provided with information in clear and plain language as to how their data is processed, as set out above (paragraph 21).

23. Data controllers should, on request, confirm if they process an individual's data, provide a copy of the data and provide detailed information about how that data is processed (**right of access**). Organisations should meet such requests within one month and without charging a fee. However, they should first consider whether the information requested constitutes personal data, and if disclosing it would breach any obligation of confidentiality or involve disclosing another individual's personal data. If so, further consideration is required. Data controllers may withhold disclosure where a request is excessive. The following link to guidance on the ICO's website will assist practices' considerations on receipt of a subject access request and includes a helpful checklist: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/ (There are certain exemptions, for example, regulatory bodies where the body's function has been conferred by legislation or is of a public nature and exercised in the public interest).

24. Data subjects are also entitled to have their personal data rectified if it is inaccurate or incomplete (**right of rectification**), and in some cases to have it deleted (**right of erasure** or "right to be forgotten"). If the data has been disclosed to a third party, an organisation must inform the third party of the rectification (or erasure) where possible. The individual must also be informed about the third party to whom their data has been disclosed.

25. In certain circumstances practices may encounter further rights that data subjects have, such as:

    a. the **right to object** to their data being processed on the basis of the practice's legitimate interests;

    b. the **right to restrict** their data being processed due to inaccuracy or an objection being raised; or,

    c. **the right to data portability**.

26. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

What does my practice need to do?

27. Firstly, ask yourself what data your practice holds/processes and why you have it/process it. Make a register of where it is, how it is stored and who is responsible for it.

28. Once completed you will be able to draft your privacy policy in accordance with the guidance from the ICO (paragraph 21).

29. If the personal data you hold is no longer necessary for the purposes you collected it for, then you should either delete it altogether or anonymise the information that would identify the person in question.

30. Where your practice uses data processors such as laboratories, or outsourced HR and payroll functions, the GDPR also requires written contracts between data controllers and processors and does not allow for a transitional period. Therefore, from 25 May 2018 existing agreements need to be amended to include processor and controller obligations such as: subject matter, duration, nature and the purpose of processing. The processor is required to maintain records of personal data and processing activities. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

31. Educate your workforce; roll out clear policies and procedures, including what to do if there is a data breach. Instil these policies from the top of an organisation down. Ensure employees are aware that non-compliance on their behalf will mean employer liability.

What to do if there is a data breach

32. The GDPR **requires mandatory notification** of a data security breach to the ICO, upon organisations, without undue delay and no later than 72 hours of becoming aware of it, unless it is unlikely to result in a risk to the relevant individuals' rights and freedoms. Late notification requires justification.

33. **Where the breach is likely to result in a high risk to a person's rights and freedoms**, eg physical harm, discrimination, identity theft or fraud, reputational damage, financial loss, loss of confidentiality and any other significant economic or social disadvantage, you must also inform the individual(s) concerned, without undue delay.

34. All breaches must be documented and actions taken should also be noted. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-breaches/

35. Non-compliance with the GDPR could lead to sizeable financial penalties. The maximum penalty is up to 4% of worldwide annual turnover or 20 million Euros for the most serious infringements such as insufficient consent to process data.

Where can I go to help me prepare for GDPR?

Summary of sources of assistance from the ICO

36. The Information Commissioner's Office (ICO) is committed to assisting businesses to prepare to meet the requirements of the GDPR. The ICO website (https://ico.org.uk) also has several online articles and checklists to help organisations prepare:

    a. Overview – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

    b. Guide on preparing for the GDPR – https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

    c. GDPR readiness quiz – https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

    d. ICO's retention policy advice - https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/

Q&As

1. Will the GDPR still apply when the UK leaves the EU?

Yes, the UK Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. Do I need to register with the ICO?

Under current data protection law, organisations that process personal information are required to notify the ICO, as data controllers (unless exempt **https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/**), and explain what personal data is collected and what is done with it. They are also required to pay a notification fee, based on their size which is currently £35 to £500. When the GDPR comes into effect there will no longer be a requirement to notify the ICO in this way, however there will still be a legal requirement for data controllers to pay the ICO the data protection fee outlined above.

3. Does the GDPR apply to data about animals?

No, the GDPR applies to data that can identify a living individual. This does not include animals.

4. How can my practice inform individuals how we process their personal data?

By ensuring that your practice's privacy notices are clear, concise, transparent and easily accessible (see paragraph 1 above). The ICO website has helpful guidance which will assist in the preparation of such a notice **https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/**

5. What does my practice do if a client makes a subject access request?

First check the request is in writing (a requirement) and then ensure you respond, ordinarily within a month. A request would most commonly be made where a person wants to see a copy of the information a practice holds about them. Paragraph 23 above contains further information on how to respond to subject access requests and a useful link to guidance from the ICO which includes a checklist of what should be considered upon receipt of a request.

6. Do I have to erase a client's data if they ask me to?

If the lawful basis for processing the data is consent, and consent is withdrawn, then you must comply with the request unless you have another legal ground for processing the data. If, however, you are processing the data on another lawful basis, you need to weigh up whether you are justified in retaining the information, or some of it (see paragraph 15 above). If in doubt, check with the ICO.

7. If a client moves to another practice does that mean that they have automatically asked to be forgotten?

No, but you should consider whether you still have a lawful basis for retaining the data such a legitimate interest, eg a potential fee dispute. (See paragraph 15 above)

8. What is a data breach?

The loss, damage or destruction of data, or the unauthorised disclosure, access or alteration of personal data, eg typing the wrong email address and sending personal data regarding Mr X to Mrs Y.

9. If there is a data breach, should I inform the individual concerned?

Yes, if the breach is likely to result in a high risk to that individual's rights and freedoms. **https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/**

10. My practice is small, is there a specific advice line for businesses like mine?

Yes the ICO has a dedicated telephone line for small and medium-sized businesses: 0303 123 1113.

11. What impact does the GDPR have on sharing of patient history when referring?

Information relating to the animals is not affected by the GDPR (see question 3 and paragraph 5 above). You will need a lawful basis for transferring a client's data, such as consent. You should be clear about what client data on file you have consent to transfer to the new practice; a client may not want you to transfer personal data relating to bills/invoices.

12. My practice is familiar with data protection law and its requirements. What is the biggest change brought about by the GDPR?

Arguably accountability. Having a lawful basis for processing data is not a new concept, but the GDPR will expect practices to show how they are compliant via their policies and procedures and how they have been implemented.

13. My practice has a Practice Management System (PMS), what should I consider to ensure it is GDPR compliant?

As with all data held, review what data is stored, why, and who has access to it. Consider how long the data is stored for. Once you have formulated your internal policy speak to your PMS provider regarding what options are available for removing or archiving data that is no longer necessary.

14. How long should my practice retain client/ clinical records for?

We do not specify a period for retention but would highlight that the indemnity insurers have historically advised such records are retained for seven years (six years is the maximum limitation period for most civil claims, plus one year). Practices will be aware that record-keeping requirements for veterinary medical products are set out within the Veterinary Medicines Regulations. Furthermore,records for the retail supply (incl administration) of POM-V and POM-VPS medicines must be kept for five years. As set out in paragraph 29 above, if the personal data you hold is no longer necessary for the specified purpose, then you should either delete it altogether or anonymise the information that would identify the person in question. If in doubt speak to the ICO and your professional indemnity insurer.

15. Do I need a Data Protection Officer (DPO)?

DPOs need only be appointed if you have over 250 employees, are a public authority, carry out large-scale systematic monitoring of individuals (online tracking etc) or carry out large-scale processing of special categories of data or data relating to criminal convictions and offences. Whilst a DPO is most likely not going to be required under the GDPR for many practices, for some it will be necessary and even when it is not, it is sensible to have somebody within the practice in charge of GDPR.

16. A client disagrees with an entry in their pet's clinical records and insists you rectify it, what do you do?

Does the entry relate to the client's animal? If the entry relates to the client's animal there is no right to rectification because data must relate to a living individual not an animal.

If the data relates to a dispute over what has been said to a client then you may wish to record the differing views or raise the matter with your professional indemnity insurer.

If, however, the data relates to your client and is inaccurate or incomplete the client is entitled to have the error rectified. You must ordinarily respond within a month (two months if a complex request).

If you are not taking action to rectify you must inform the individual concerned as to why and advise that they may complain to the supervising authority, the ICO.

17. When a client signs up for the practice can I ask them to consent to receiving reminders and special offers?

Yes, but remember, consent must now be freely given, specific, informed and an unambiguous indication of an individual's wishes in order to comply with the GDPR. Consent requires a positive opt-in. You cannot use pre-ticked boxes or other methods of default consent. Consent also cannot be implied and must also be separate from other terms and conditions. Practices should make it simple for consent to be withdrawn. Keep consent under review and refresh it if anything changes.

18. Are there different rules if I send leaflets in the post to sending text messages and emails?

Yes, specific consent must have been obtained from the individual concerned in order to direct market via phone calls, text messages and emails. However, if you do not have consent, the solution is not to email all your clients to ask for consent to email/text marketing, as this in itself is likely to constitute email marketing, and therefore breach the GDPR and the current Privacy and Electronic Communications Regulations 2003 (PECR) - https://ico.org.uk/for-organisations/guide-to-pecr/. Instead, you could ask clients to 'opt in' by ticking a box on a form when they next come to the practice, or on a leaflet that you send by post. You should keep records of such consents, including when they were given and exactly what they covered.

19. A client caused trouble at the practice and I want to make a note to 'warn' colleagues – am I allowed to do this?

Yes, however personal data from which a client is identifiable may be the subject of a subject access request and could be disclosed to the client on receipt of such a request.

20. What about if a client has health difficulties that impact on their caring for their pet and I want to record this so that all members of staff are aware even if I am not there. Can I do it?

Yes, but as this falls into special category data (see paragraph 8 above) you should first obtain the explicit consent of the client (see paragraph 12 above).

21. I've asked my clients to opt-in to consent to vaccine reminders. I know that consent does not last forever, but how often do I need to ask?

You are not required to refresh all existing DPA consents in preparation for the GDPR. If you rely on an individual's consent to process their data, make sure it meets the GDPR standard on being; specific, clear, opt-in, properly documented and easily withdrawn.

If the consents you previously obtained do not comply with these standards, or you have not heard from the client for some time, you should consider refreshing consent. There are no hard and fast rules about how often this should be done, however an annual refresher would not be disproportionate. All communications and the vaccine reminders themselves should include an opt-out.

If you do not already have consent to send vaccine reminders, such consent will need to be obtained. However, do not email or text all your clients asking for consent, as this may be considered as unsolicited email marketing (see question 18). If in doubt, contact the ICO.

22. We have a number of contracts that have been running for years where we pass data to other third parties, eg outsource payroll or reminder services. Can I assume that these contractors/data processors are doing everything ok? And who is responsible if something goes wrong?

No, you cannot assume everything is ok. The GDPR requires written contracts between data controllers and processors and does not allow for a transitional period. Therefore, from 25 May 2018, existing agreements need to be amended to include processor and controller obligations, such as: subject matter, duration, nature and purpose of processing, as well as confidentiality and security etc.

The processor is required to maintain records of personal data and processing activities. The ICO has provided a helpful checklist to help in the drafting of such contracts - **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/**

Whilst data processor obligations have been increased, this does not decrease the obligations on data controllers. Small and medium sized practices may want to consider asking processors to provide a contract for review and then consider it against the checklist set out within the link above on the ICO's website.

23. Can I ask a client to agree to give consent up front in the event that they want to change practice and I can then transfer contact details, so that I do not have to do it at the time when they have gone to visit another vet?

Yes, provided the GDPR standards on consent are met, namely the consent is specific, clear, transparent, opt-in, properly documented and easily withdrawn. If you do not have such consent and your client wants you to transfer their records to another vet, it is likely you will obtain consent at this stage. If in doubt, obtain such consent before transferring such personal details.

24. When someone 'opts in' and consents, does this always have to be in writing?

No, however, for consent to be GDPR-compliant, there must be some form of clear affirmative action, namely a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity. Clear, concise and properly documented consent will remove ambiguity and ensure compliance.

As the GDPR makes consent more difficult to obtain, verbal consent should be recorded clearly, concisely and properly to remove ambiguity and ensure compliance. A record should be kept of what information was given to the individual, so that you can demonstrate that the consent was specific and informed (as required by the GDPR).

25. What if I want to transfer data to debt recovery agents?

The sharing of client data with a debt recovery agent will not require the client's consent as the practice will have a legitimate interest in sharing the data and therefore will have a lawful basis for, doing so.

26. I like to circulate electronic client surveys to get feedback on how we are doing as a business. Can I do this?

It could be argued that practice feedback forms do not constitute marketing material, and that you have a legitimate interest in collecting feedback. However, to avoid criticism, practices could obtain consent to obtain feedback yearly or after appointments. Ideally, obtain consent in person when the client visits the practice, not by email (which could be considered as unsolicited marketing in itself). Practices should be mindful of electronic marketing requirements (see question 18), which can be avoided by sending feedback forms by post.

27. I am involved in the data management and storage of data for research purposes. What should I be aware of?

If you are storing or managing personal data which has undergone 'pseudonymisation', and which could be attributed to an individual by the use of additional information, the principles of the GDPR set out in the above statement apply to that information. In helping you to determine whether a person is identifiable, you should take account of the means likely to be used to identify the person directly/indirectly, for example cost and technology.

The principles of data protection do not apply to truly anonymous information, namely information which does not relate to an identified or identifiable person, or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable.

28. Under existing employment legislation, I am required, for example, to retain accident reports for three years and salary records for six years. Is this still applicable?

The GDPR does not specify particular retention periods for personal data, but states that it should be kept, in a form that permits identification of an individual, for no longer than is necessary for the purpose for which it was processed.

Practices may be guided by statutory retention periods, limitation periods and business needs. Therefore, when formulating practice policies and procedures, have regard to current legislation which sets out retention periods for Human Resources data.

29. Does my practice need an information asset register? If so, what are the minimum requirements?

In conducting your data audit in which you set out: the type of personal data held, how and why it is processed, where it is stored, who has access to it, where it is transferred (if applicable) and when it is deleted, you will compile the basis for your asset register. In doing so, your practice will also be helping to demonstrate how it complies with the GDPR, and identifying any issues which need to be addressed to ensure compliance.

30. What impact will the GDPR have on consent in terms of the client relationship, when the owner and client are not the same person?

Practices should have regard to chapter 11 of the supporting guidance to the RCVS Code of Professional Conduct on communication and consent – **www.rcvs.org.uk/consent** – which states that care should be taken in situations where the client presenting the animal is not the owner.

With regards to processing personal details, practices should remember that they require consent or another lawful condition in order to process personal data (see paragraph 14 above).

Clear, concise, transparent and well documented consent will assist in ensuring compliance with the GDPR, but in situations where you may have to process Mr X's personal details when Mr Y is presenting Mr X's animal and you are uncertain as to whether you have Mr X's consent, do check. Remember, consent cannot be implied. If you are taking Mr Y's personal details as well, you will probably need his consent because you will not be performing a contract with him.