Data Protection Tick-list

For Vets

Version 1.1 - 8th Decemeber 2017

Introduction to this **Data Protection Tick-list**

This tick-list is one of the 'Three routes towards General Data Protection Regulation (GDPR) compliance' that are being published by Connected Vet in association with SPVS.

This tick-list is based on the Information Commissioner Office's (ICO) **'12 steps to prepare for the GDPR'** guidance. It has been designed to make the ICO's information more relevant to independent veterinary practices.

Format

This document lays out the ICO's recommended 12 steps to prepare for the GDPR but it does it in an order that we think is more relevant to vets.

We have tried to add practical help and examples (that are not available as far as we can see in the ICO's resources) that make this document specifically relevant to vets. In complementing the ICO's material this document in part necessarily comprises of opinions based on the experience of conducting data privacy protection work in practices. That in turn means that a practice should not rely on this tick-list as a legal basis for completing your own practice's data protection work.

We aim to regularly update this document so please do refer back to it from time to time.

Note: Neither Connected Vet nor its partner organisations will accept any responsibility for losses arising from the use of the information in this document. This document should not be regarded as constituting legal advice and should not be relied on as such.

Introduction to GDPR

Whilst many of the General Data Protection Regulation's (GDPR) main concepts and principals are much the same as those in the current Data Protection Act (DPA), most veterinary practices in the UK have a low level of awareness of the DPA and therefore probably have little insight into their practical compliance with the current legislation.

This means that, like many other businesses in other sectors, the enforcement of the GDPR on **25th May 2018** will make most veterinary practices do some things for the first time and some things differently. Most practices in the UK will almost certainly need to focus more resource on the way they manage data protection as a business issue. It is important that practice owners, directors and principles consider their options and make a plan to ensure their practice has a planned a route to compliance sooner rather than later.

This tick-list, forms the basis of what we consider to be an 'Unassisted' route. It is designed to signpost veterinary practices to generally available resources to work out what they need to do. The ICO regularly produces new guidance and other tools to assist you, if you choose this route you should review the ICO's resources regularly as they are frequently updated.

People and their personal privacy are at the heart of this new legislation and this thought should be at the heart of everything a veterinary practice does. If you take a people first approach to the management of personally identifiable information (PII) within your practice then you will naturally begin to build the culture of privacy that the ICO is seeking to promote with the introduction of this legislation.

DEADLINE 25 May 2018

1

Awareness

You should make sure that decision makers and key people in your practice are aware that existing law is changing to accommodate the GDPR. The new law demands that your practice owners, directors or principals are accountable for the personal data they hold and take steps to appreciate the impact that holding this data may have.

To be properly accountable anyone should understand the implications of implementing the **six privacy principles.**

These are...

1. Lawful, transparent and fair
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

Once you understand these you must identify areas that could cause compliance problems under the GDPR and work to mitigate any risk.

The ICO has warned that businesses may find compliance difficult if they leave preparations until the last minute.

1. Your practice owners need to find out about their responsibilities. This will be easier if they research & understand:

- The 6 privacy principles
- The 6 lawful basis for processing
- The 8 rights of data subjects

2. Practice owners, directors or principals must take action to ensure that your business processes around personal data are compliant.

3. Your practice owners, directors or principals should make a plan now for how the business will become compliant.

Handy documents

The ICO's website offers further advice on making sure owners are accountable for the personal data that their business holds. You can access that advice at http://bit.ly/2BK8LWk

2

Information you hold

Your practice should document what personal data you hold, where it came from and who you share it with. You will probably need to organise a data audit across the practice.

The GDPR requires you to maintain records of your processing activities. For example, if you have inaccurate personal data and have shared this with another practice (for instance when you transfer PII) you will have to tell the other practice about the inaccuracy so it can correct its own records.

You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this.

Documenting your personal data will also help your practice principals to comply with the GDPR's accountability principle, which requires practices to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

Documenting your personal data will also help your practice principals to comply with the GDPR's accountability principle, which requires practices to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

1. You need to document the personal data your practice holds and where it is stored.

2. You need to document where that personal data comes from.

3. You need to document the processes you use to gain, store, change and dispose of that personal data.

4. You need to document who you share that personal data with and any suppliers that help you manage and process that data.

5. You need to document which of the six legal basis you are relying on to gather, hold, manipulate, send and store each category of personal data you hold.

Handy documents

The ICO has produced a checklist for Data Controllers that will help you complete this section. You can access it here http://bit.ly/2nLOTzK

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice.

Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data.

The GDPR requires the information to be provided in concise, easy to understand and clear language.

1. Your practice will need to review its current privacy statement (normally found at the foot of your website) to check it meets the new standards.

2. You'll need a plan to update the bits of the notice that do not meet the new standards.

3. You'll need to ensure you also show that information in other appropriate areas of your website and other digital channels.

4. You can really only produce an effective privacy statement once you have completed a data audit.

5. It's not wise to simply copy another practice's privacy notice. They will almost certainly do certain things in a different way to your practice.

Handy documents

The ICO has produced a guide that reflects the requirements of the new privacy notice. You can see the guide here
http://bit.ly/2B2NAS5

4

The rights of the individual

You should check your procedures, or create some if you have none, to ensure you have a policy that covers all the new rights individuals have, including how you would delete personal data or provide personal data electronically and in a commonly used format.

The eight rights of the individual are;

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object and
8. The right not to be subject to automated decision making.

On the whole, the rights individuals will enjoy under the GDPR are similar to those under the DPA but with significant enhancements.

This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new under GDPR. It only applies to personal data an individual has provided to you and where the processing is based on the individual's consent or for the performance of a contract.

1. You need to consider whether you need to revise or create policies and or procedures to accommodate the rights of individuals.

2. Most veterinary practices we have seen do not historically have these.

Handy documents

The ICO provides specific information on the eight rights of the individual. You can access it at http://bit.ly/2iCcIoc

5

Subject Access Requests (SAR)

You should update your practice procedures and plan how you will handle requests from individuals to take account of the **new rules:**

These are...

1. In most cases you will not be able to charge for complying with a request.
2. You will have a month to comply with a SAR rather than the current 40 days.
3. You can refuse or charge for requests that are manifestly unfounded or excessive.
4. If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy.
5. You must do this without undue delay and at the latest, within one month.

You should consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

1. Your practice will need a procedure to handle Subject Access Requests.

2. You'll need to train appropriate staff to be able to deal with Subject Access Requests. This is most likely to be (but may not be limited to) customer-facing staff – especially receptionists.

3. Your practice will need to understand when and how to turn down a Subject Access Request and the options you need to make the individual aware of at the time you do so.

4. The practice must be able to provide additional information upon request regarding access to personal data.

Handy documents

The ICO has produced a checklist to help you handle Data Subject Access Requests. You can see the checklist here http://bit.ly/2AtVIMl

6

The lawful basis for processing personal data

You should identify the lawful base for your processing activity in the GDPR, document it and update your privacy notice to explain it. The six lawful basis for processing data under the GDPR are:

These are...

1. Contractual obligation
2. Legal obligation
3. Vital interest
4. Public interest
5. Legitimate interest
6. Consent

Many practices will not previously have considered their lawful basis for processing personal data. Under GDPR some individuals' rights have been strengthened depending on your lawful basis for processing their personal data. So, it's important that your understanding is good.

The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful base for processing personal data in your privacy notice and when you answer a subject access request. It should be possible to review the types of processing activities you carry out and to identify your lawful base for doing each type. You should document your lawful basis in order to help you comply with the GDPR's 'accountability' requirements.

1. You'll need to identify the lawful basis your practice is relying on to collect, store, manipulate, send and delete each class of personal data that you hold.

2. Your practice will need to update its privacy notice to reflect the lawful basis on which you are relying and for what.

Handy documents

The ICO has produced specific guidance on the lawful basis for processing individuals' personal data. You can access it here http://bit.ly/2iDiiHf

7

Consent

If you choose to rely on consent then it must be freely given, specific, informed and unambiguous. There must be a positive opt-in as consent cannot be inferred from silence, pre- ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent.

You are not required to automatically 'repaper' or refresh existing consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it meets the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn.

If you don't currently meet these standards then alter your consent mechanisms and seek fresh GDPR-compliant consent, or better still justify an alternative legal base.

1. Your practice will need to be very clear on when consent is required.

2. You'll need to record how you seek, record and manage consent if your practice intends to rely on it as a lawful basis for using individuals' data.

3. Practices will need to make sure that it is easy for individuals to withdraw their consent.

4. You absolutely MUST make sure that if you are using consent that it was gained in a physically different place to any other information.

5. You may want to see if your current consents are capable of being updated rather than re-papered, that may save your practice time.

Handy documents

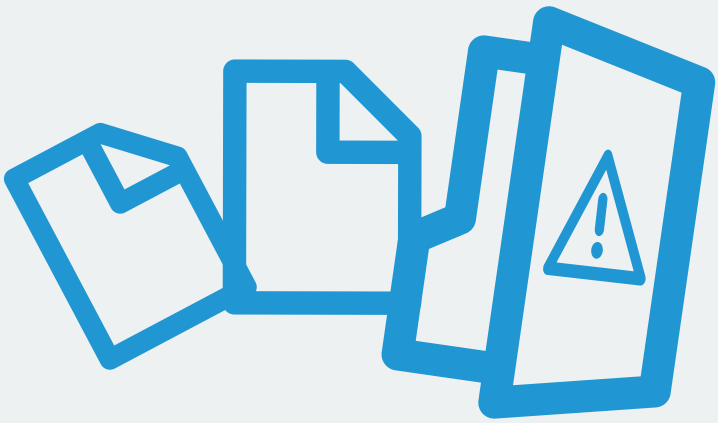
The ICO has produced detailed guidance on consent that will help ensure you are more rather than less compliant.
http://bit.ly/2BdCqe6

8

Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

The GDPR introduces a duty on your practice to report certain types of data breach to the ICO, specifically where the breach is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in damage to reputation or financial loss or any other significant economic or social disadvantage.



Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will have to notify the individuals concerned directly.

You should assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. This is best done as part of your data audit.

Larger practices will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

1. The practice will need to make sure it has processes in place to detect personal data breaches.

2. You will also need to understand when, how and to whom you need to report data breaches.

3. Finally you'll need a system in place to remediate the causes of any data breaches to ensure they don't re-occur.

Handy documents

The ICO has produced this useful video on detecting and managing data breaches. You can watch it here https://youtu.be/XuwHJhOZELc

9

Data protection by design & Data Protection Impact Assessments

It has always been good practice to design data privacy into any system your practice has that handles the personal information of individuals. This is called 'Data protection by design'. It's also good practice to carry out a Privacy Impact Assessment (PIA), the personal data equivalent of a risk assessment, in certain circumstances.

The GDPR makes privacy by design an express legal requirement. It also makes Data Protection Impact Assessments (DPIAs) mandatory in certain circumstances. A DPIA is mandatory where data processing is likely to result in high risk to individuals. If you cannot sufficiently address the high risk, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should assess the situations where it will be necessary to conduct a DPIA as part of your information audit. You should also familiarise yourself with the guidance the ICO has produced on PIAs to work out how to implement them in your organisation.

1. Data Protection Impact Assessments within the GDPR are similar to Risk Assessments within health and safety legislation. You'll need to understand when your practice needs to complete one.

2. The circumstances in which your practice will need to complete one will be identified in the data audit.

3. You'll then need to ensure your practice is familiar with the ICO's code of practice on how to undertake Data Protection Impact Assessments.

4. Finally you'll need to understand what you need to do if the DPIA exposes a risk to an individual's personal information that cannot be quickly mitigated.

Handy documents

The ICO has produced a comprehensive code of practice on conducting Data Protection Impact Assessments. You can download it here http://bit.ly/2nNnzkY

10

Data Protection Officers & Data Protection Managers

Your practice should designate someone to take responsibility for data protection compliance and the owners of the business should assess where this role will sit within your practice's structure and governance arrangements.

As part of your information audit you should consider whether you are required to formally designate a Data Protection Officer (DPO). If you do not appoint a DPO (the most likely situation for small independent vets) then it would be good practice to assign a member of the team to manage your practice's compliance. You should call this individual a Data Protection Manager, or something similar, to distinguish them from the statutory role of a DPO.

It's vital that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge and support to carry out their role effectively.

1. Your practice needs to designate an individual who will take responsibility for data protection compliance. You might call them a Data Protection Manager.

2. Whilst most small to medium sized practices will probably not need a DPO, you should document your reasons for not appointing such an individual.

3. Practice owners should understand the practical statutory differences between a DPO and a DPM.

4. When you have appointed a DPO or a DPM you'll need to ensure that there are processes in place to help them do their job properly.

Handy documents

The Article 29 Working Party has produced guidelines on when to appoint DPOs and how they should operate. You can find them here http://bit.ly/2A57QDs

Children & International

The final two sections deal with the personal data of children (under 16s) and data that will cross international borders.

Unless your practice holds the data of children or manages personal data across international borders this section may not be so relevant to you.

11

Children

For the first time, the GDPR will bring in special protection for children's personal data.

Whilst most practices won't hold the personal data of children, if your practice does then you should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

The GDPR sets the age when a child can give their own consent to processing of their personal information at 16 (although this may be lowered to a minimum of 13 in the UK as part of the new Data Protection Act currently working its way through the parliamentary process). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your practice offers online services to children (can they book online for puppy parties or kitten clinics) and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

1. Your practice will need to have a system in place to verify an individual's age.

2. You'll also need a system for gaining parental consent in the unlikely event that you are processing children's personal data.

Handy documents

Get the ICO's guidance on dealing with the personal data of children here
http://bit.ly/2j4vvg7

12

International

If your practice operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

1. If your practice works in more than one EU member state then you'll need to determine & document in which state you handle most of your personal data.

2. You'll then need to determine who your lead supervisory authority is.

3. Once your practice understands this you'll need to understand how you should deal with personal data that is spread across multiple states.

Handy documents

The Article 29 working party (an EU body that is publishing guidance on implementing the GDPR) has produced guidance on how to identify your lead supervisory authority. You can download that here http://bit.ly/2jPIi26

FAQs

Information Commissioner's Office

The ICO has produced a general list of GDPR FAQs for small to medium sized business, which you can access here http://bit.ly/2kwz7HZ

CONNECTED Vet

Connected vet has published a list of FAQs that it has dealt with on its regular GDPR webinars. These are regularly updated and can be accessed here Needslink-http://bit.ly/2kwz7HZ

And finally....This is just the start

We hope you have found this document useful. In reading it you accept that this tick-list is a general document and we strongly recommended that you should consult the ICOs website, and/or, seek independent specialist advice in order to effectively apply elements of this document to your practice's individual circumstances.

Neither Connected Vet nor its partner organisations will accept any responsibility for losses arising from the use of the information in this document. This document should not be regarded as constituting legal advice and should not be relied on as such.

Whilst we will attempt to keep this document up to date, the law regarding GDPR is constantly evolving and you should use the links to ICO resources as a starting point for wider reading if you intend to manage your practice's own route to compliance unassisted.