### General Data Protection Regulation (GDPR) checklist for veterinary practices

**BVA workplace guidance | March 2018**

If you tick a shaded box, you need to put measures in place so that you can change your response.

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you registered with the Information Commissioner’s Office as a Data Controller?</td>
<td></td>
<td></td>
<td>Any organisation collecting personal information should be registered with the Information Commissioners Office. It is £35 per year.</td>
</tr>
<tr>
<td>Have all staff received training for confidentiality or data protection over the last year?</td>
<td></td>
<td></td>
<td>It is good practice for all staff to receive confidentiality training at least annually.</td>
</tr>
<tr>
<td>Has the training undertaken been documented?</td>
<td></td>
<td></td>
<td>Any training for data protection should be documented so you can prove to the Information Commissioners Office that it is taking place.</td>
</tr>
<tr>
<td>Do all staff sign a confidentiality clause as part of their employment?</td>
<td></td>
<td></td>
<td>There should be a confidentiality clause in your employment contract.</td>
</tr>
<tr>
<td>If using a customer database – is access restricted with the use of passwords etc?</td>
<td></td>
<td></td>
<td>Any database storing personal information should be password protected.</td>
</tr>
<tr>
<td>Have you obtained appropriate customer consent to text your clients?</td>
<td></td>
<td></td>
<td>If you are texting your clients, you need specific consent to do so.</td>
</tr>
<tr>
<td>Have you obtained consent to contact your clients by phone?</td>
<td></td>
<td></td>
<td>Have you asked for permission to contact clients by phone? It's a requirement of the electronic communication regulations.</td>
</tr>
<tr>
<td>Question</td>
<td>Yes</td>
<td>No</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Do you have a retention policy outlining how long information will be</td>
<td></td>
<td></td>
<td>A retention policy should be established outlining the periods you will retain various records. The period will vary depending on the record. There are some good practice periods such as 7 years for accounting records.</td>
</tr>
<tr>
<td>retained and how it will be destroyed?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a data protection policy setting out your data protection</td>
<td></td>
<td></td>
<td>Create a simple data protection policy which sets out how you handle personal information. This should be available to both staff and clients.</td>
</tr>
<tr>
<td>practices?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are staff personal files held securely?</td>
<td></td>
<td></td>
<td>Staff files should be secure and accessed only by those who need to see them or action them.</td>
</tr>
<tr>
<td>Do you have written agreements with contractors who have access to</td>
<td></td>
<td></td>
<td>It is a requirement of the General Data Protection Regulation that any subcontractor is subject to a written agreement which should outline their responsibilities and how they will ensure the security of the personal information shared with them.</td>
</tr>
<tr>
<td>personal information you are collecting? Such as debt collectors,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>locums, agency staff?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there clear collection notices or statements provided at the time</td>
<td></td>
<td></td>
<td>At the point you collect information, there should be a clear statement showing what that information will be used for, who it will be shared with and how long it will be held.</td>
</tr>
<tr>
<td>personal information is provided to your veterinary practice?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are emails with sensitive personal information (health and wellbeing</td>
<td></td>
<td></td>
<td>Email is like a postcard and can be intercepted en route, you therefore need to take special precautions when emailing sensitive personal information.</td>
</tr>
<tr>
<td>etc) encrypted or password protected?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are staff using their own mobile phones, tablets or computers to access</td>
<td></td>
<td></td>
<td>How do you ensure that the information on those phones is secure? Are phones locked when not in use? Is two-factor authentication in place where they have access to the client database? If the phone was lost or stolen, how much access would be gained to your systems?</td>
</tr>
<tr>
<td>practice data?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Would you know how to handle a subject access request?</td>
<td></td>
<td></td>
<td>Subject Access Requests can vary in complexity and there should be a process in place to respond appropriately to a request.</td>
</tr>
<tr>
<td>Would staff recognise a request to see the information held about an</td>
<td></td>
<td></td>
<td>Staff should be aware what a subject access request looks like so they can pass it to the appropriate person for response. This should be covered as part of your annual data protection training.</td>
</tr>
<tr>
<td>individual</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is any cloud storage you use based in the EEA?</td>
<td></td>
<td></td>
<td>The EEA is a group of countries where there is adequate security in place to protect personal information. If your cloud storage is outside the EEA, then there needs to be specific contract conditions or other measures in place.</td>
</tr>
<tr>
<td>Are practice laptops and removable media (USB drives) encrypted?</td>
<td></td>
<td></td>
<td>Where a laptop contains personal information, it is good practice to have the laptop encrypted, so if it was lost or stolen, the information on the laptop would not be accessible.</td>
</tr>
<tr>
<td>Are all software programmes hosted in the EEA</td>
<td></td>
<td></td>
<td>As with cloud storage if your software is hosted outside the EEA, then you will need to ensure that there is appropriate security or contract terms in place.</td>
</tr>
<tr>
<td>Question</td>
<td>Yes</td>
<td>No</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Have you documented the personal information that the practice collects?</td>
<td></td>
<td></td>
<td>A data audit will identify what information you are collecting, where it is held, the reason you are holding it and the legal basis for holding that information. This helps to understand the information in your practice and make sure it is secure.</td>
</tr>
<tr>
<td>Are paper files containing personal information held securely?</td>
<td></td>
<td></td>
<td>As with electronic files, paper files should be securely held too.</td>
</tr>
<tr>
<td>Do you know what constitutes personal information under GDPR?</td>
<td></td>
<td></td>
<td>This is the basic of all information. For example, things such as name, address, email address, telephone number, date of birth and IP address are all personal information. Anything that can be used to identify an individual. There is a comprehensive list on the ICO website.</td>
</tr>
<tr>
<td>Do you know what constitutes sensitive or special category personal information under GDPR?</td>
<td></td>
<td></td>
<td>This is information such as race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.</td>
</tr>
<tr>
<td>Do receptionist and those taking telephone calls take steps to protect the privacy of the person they are talking to?</td>
<td></td>
<td></td>
<td>How do receptionists protect the identity of callers, if they can be overheard in the waiting room?</td>
</tr>
<tr>
<td>Do you know what you need to do in the event of a data breach?</td>
<td></td>
<td></td>
<td>There are obligations for reporting and handling a data breach so you should have a process in place to ensure you can meet your legislative requirements.</td>
</tr>
<tr>
<td>Do you review the personal information you hold on a regular basis to ensure it is accurate and up to date?</td>
<td></td>
<td></td>
<td>The personal information that you hold should be accurate and up to date. How do you ensure that is the case? Are you checking on client contact that the address and phone number are accurate?</td>
</tr>
<tr>
<td>Is the privacy policy on your website GDPR compliant?</td>
<td></td>
<td></td>
<td>There are new guidelines about privacy policies and any website now must give some specific information so make sure your privacy policy is up to date.</td>
</tr>
<tr>
<td>If you are using CCTV in your practice, are the recordings appropriately secured?</td>
<td></td>
<td></td>
<td>You should have a CCTV code of practice which identifies the reason for using CCTV, how images can be viewed and by whom, and the retention period.</td>
</tr>
<tr>
<td>If you are recording telephone calls, is this clearly stated?</td>
<td></td>
<td></td>
<td>If you are recording telephone calls, this should be obvious to someone telephoning your practice. You should also have a clear policy about recording calls.</td>
</tr>
<tr>
<td>Do your current contracts provide adequate security for personal information?</td>
<td></td>
<td></td>
<td>If your IT is outsourced or any part of your practice where personal information will be shared is accessible, the contract in place should have some key clauses to ensure the security of the personal information that is accessible.</td>
</tr>
</tbody>
</table>

Further information
This checklist is a basic start to help you with GDPR compliance. It cannot cover all eventualities and you therefore may need to seek further advice. For further information go to www.bva.co.uk/gdpr or visit the website of the Information Commissioner’s Office at https://ico.org.uk/. For specific advice call the ICO’s helpline on 0303 123 1113.