

**MARCH 2017**

**GENERAL DATA PROTECTION REGULATION ACTION PLAN FOR PRIMARY CARE**

Themes of the GDPR:

* Refining/tightening up of existing concepts
* Standardised law across the EU
* New concepts in regulation; accountability, demonstrating compliance, designing compliance
* Increased regulation/enforcement by ICO and data subjects
* Enhanced rights for data subjects
* Expectations of uniformity and portability

GDPR comes into force on the 25th May 2018 and it is anticipated that the UK will still be a member state of the EU at that time. General opinion is that even if it was decided not to adopt the GDPR we would have to have the equivalent law in place.

While we wait for a government commitment to implementing the GDPR in the UK we do anticipate further guidance from the Information Commissioners Office but it is not known when this will be.

This action plan will start to address the main issues and map out where changes need to be made.

|  |  |  |
| --- | --- | --- |
| **Steps to take now** | **Items to be aware of** | **Actions** |
| **Raising Awareness** | * Initial comms to Primary Care
* Action plan to be agreed by practices – appoint lead
* Inform staff about new fine levels – easier for data subjects to make a claim. Can be fined even if no harm has occurred, need to be able to demonstrate compliance. Comms to staff
* Ensure accountability can be proven
 | Completed by eMBEDOrganisations to maintain records of processing activities – ongoing monitoring, reviewing and assessing processing activities to ensure compliance |
| **Information you hold** | * No longer a requirement to register with the ICO – however each controller must keep records of its processing activities – these must be disclosed to the ICO on request
* Comprehensive data flow mapping to include:

What you holdWhere it came fromWho you share it withLegal basis for processing* Information Asset Register updated regularly
 | Ensure that all areas map information and add in any new flows as they ariseConfirm the conditions being relied on, i.e legal basis, for processingEnsure that all Information Asset Owners are updating the register and risk assessing existing and new assets |
|  **Individuals’ rights** | Check procedures and policies and systems to ensure all the rights individuals have are covered including how to delete personal data or providing data electronically.  | Identify which procedures/policies require updating and the content and timing of updates  |
| **Subject Access Requests****(SARs)** | * Review and update Subject Access Procedures – no fees, time reduced to 1 month to respond
* Ensure all staff dealing with SARs are aware of the new procedures
* Need to explain legal basis for processing information and retention periods when responding to SARs (in addition to Privacy notices)
 | To be in place by 25/5/18 – advise relevant staff |
| **Legal basis for processing personal data** | Ensure all processing of data has a legal basis | Should be identified in data flow mapping |
| **Consent** | Consent must be explicit and requires clear affirmative action. It cannot be implied. A full record must be kept. Silence, pre-ticked boxes, inactivity or failure to opt-out do not constitute valid consent. Consent to the processing of personal data must always be clearly distinguished from other matters (e.g. cannot be wrapped up in other terms and conditions / consent to treatment etc.) Previously obtained consent will remain valid as long as it meets the GDPR standard* Review of all areas where consent is used as the legal basis for processing and ensure adequate processes are in place
 | Identify all areas using consent as legal basis for processing and look at alternatives |
| **Children** | * Ensure that processes are in place for recording consent of parent or guardian where appropriate (children under 13)
* Add in section to Privacy Notice in a clear, plain way that a child can understand about their consent or produce separate notice for children
 | Organisation to ensure processes are in placeOrganisation need to identify whether necessary |
| **Data breaches** | Ensure that all staff are aware that breaches must be reported within 72 hours and that there is a new duty to inform data subjects of high risk breaches. Comms to staffEnsure incident reporting policy and procedures are clear and well-practised to ensure quick response to any breaches – note fines now up to €20,000,000Data subjects have the right to compensation from a data controller or data processor | Ensure processes are in place and all staff are made aware. Review incident reporting policy and proceduresOrganisations to ensure all processors have contracts in place and are IGT level 2 compliant |
| **Data Protection by Design and Data Protection Impact Assessments** | Embed the Privacy Impact Assessment process within the organisationAny new systems should be commissioned and built using data protection by design and by default.Requirement to consult with the ICO in advance where a data impact assessment indicates that the processing would result in a high risk ifmeasures are not taken to mitigate that riskCCTV or health monitoring systems must have a PIA | PIAs to be completed for all new systems or processes involving patient identifiable data.IT and commissioning teams need to be aware |
|  **Data Protection Officers** | All public bodies and organisations that carry out large scale processing of data (such as health data) must have a data protection officer who takes responsibility for data protection compliance* Must have expert knowledge
* Must report directly to the board or equivalent

Must be independent (can be a contractor) – a group of public authorities may collectively appoint a single DPO (as long as the DPO is accessible to all) | Practice to appoint but need more detail on who this should be |
| **New duties for data processors** | * Data processors become data controllers if they act beyond instructions
* Restrictions on sub-contracting by data processors
* Must have clear contractual provisions
* Data processors can now be fined
 | Check all existing data processor contracts for compliance.Check who has access to systems. |
| **Fair Processing Notices** | Must be transparent and easily accessible. Concise form. Must include:* Contact details of the data controller
* Contact details of the Data Protection Officer
* Schedule 2 and 3 conditions relied on
* Data retention period
* Reference to the rights of erasure, rights to withdraw consent, to object to processing, data portability and to complain to the ICO

Revisit fair processing notices for staff – don’t rely on consent | Review whether separate privacy notice is required for childrenWhere records are held areas to check data retention periods as these will need to be added inReview data sharing agreements to ensure data subjects are being provided with all the relevant informationReview contracts |
| **Audits** | Additional powers granted to the ICO will allow them to:* Carry out audits
* Issue orders to cease operations
* Notify data subjects of a breach
* Restrict or erase data
* Suspend or prohibit processing or order suspension of data flows to third countries

Need to ensure all the above actions are completed before May 2018 | Organisations need to ensure that they can demonstrate compliance in all areas of the GDPR – with **evidence** that it is meeting its obligations |