

EMIS Group and the GDPR (General Data Protection Regulation)

What is GDPR?

Each member state in the EU operates under the current 1995 data protection regulation and has its own national laws. In the UK, the current Data Protection Act 1998 sets out how your personal information can be used.

The General Data Protection Regulation (GDPR) changes how data can be used and is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen data protection. Companies who hold or process data need to be compliant with the GDPR regulation by 25 May 2018.

What is EMIS Group doing about this?

As an organisation we take issues of information governance and data privacy very seriously and have them at the heart of what we do. Some of what we're doing to ensure compliance with the new regulation is commercially sensitive, however we can confirm we have a project team in place who are currently working on a project plan to ensure that we're compliant.

We are happy to share with you the following high level overview of some of the steps we're taking to address the forthcoming changes in data privacy law:

Raising awareness

We're raising awareness of information governance issues across the group through: the delivery of bespoke training, training modules, use of our internal newsletters and the revised IG toolkit made available by NHS Digital.

We're revisiting our data breach management policy, including arrangements for compulsory breach notification, so that staff know who to contact should an incident arise.

We will engage with sector specific bodies active in setting standards (e.g. the Information Governance Alliance) so that we are aware of any relevant industry codes of practice.

Product Development

We're engaging with our product development teams to identify those elements of the GDPR which

we believe may have impact on solution design going forward.

We're revisiting our data protection impact assessment process to ensure that PIA's are undertaken as required.

Review Data Security

We recognise the need to meet the integrity and confidentiality principles under the GDPR. Therefore we're reviewing the below to ensure that they are fit for purpose:

- Data security standards.
- Data breach, storage and destruction policies and management.
- Data security action plan.

Data Protection Officer

We will be appointing a Group DPO with overall responsibility for compliance.

Policy & Contract Review

We're reviewing and updating the below to ensure that they are fit for purpose:

- Data privacy related policies and procedures.
- Data sharing agreements and process.
- Fair processing notices (privacy policies) & website terms.

We will review and revise as appropriate our own terms and conditions and those put forward by our customers so that they reflect the requirements of the new regime.

Useful links

- [NHS Digital guidance](#)
- [ICO health-specific guidance](#)
- [NHS Employers guidance](#)
- [Guidance on consent](#)
- [Guidance on lawful processing](#)