EDGE and the GDPR (General Data Protection Regulation).

Summary

With the draft implementation of the GDPR (General Data Protection regulation) moving into law on the 25th of May 2018 the Clinical Informatics Research Unit (CIRU) at the University of Southampton (UoS) have produced this document to support the transition for our subscribing organisations.

The document seeks to clarify how CIRU is preparing for the changes in law and explain how the EDGE service meets the Draft Guidance which sets out the requirements on contracts and liabilities. It also explains details of how GDPR will affect our department as Data Processors and our EDGE subscribers, as Data Controllers. It includes answers to some frequently asked questions and where to find the information you'll need.

Background

On the 13th September 2017, the Information Commissioners Officer (the "ICO") commenced a consultation on draft GDPR guidance on contracts and liabilities between controllers and processors.

With significant advancements in the field of information and communication technology and the growth in network interoperability (such as the internet, globally distributed corporate networks and the cloud), the ease with data which may be collected, transmitted, stored, manipulated and most importantly disseminated has rapidly increased. These developments, together with a general increase in awareness of fundamental rights, particularly the right to privacy, have led to legislative changes and the emergence of a new regime of privacy protection.

The ICO noted that the GDPR builds on the existing requirement of "Principle 7" of the Data Protection Act 1998, to have a written contract in place between a controller and a processor, and that the GDPR requires more specificity in these contracts; it specifies the terms such as setting high standards and protecting the interests of data subjects.

Clinical Informatics Research Unit
NHSBT Southampton, MP852
Southampton General Hospital
Coxford Road, Southampton, SO16 5AF

t +44 (0) 2382 02 7200
e edge@soton.ac.uk
w www.edgeclinical.com
tw @EDGEclinical

BREXIT and GDPR

The GDPR will become directly applicable on 25 May 2018 before the UK leaves the EU (scheduled for 29 March 2019). Once the UK leaves the EU it will become a "third country" for the purposes of personal **data transfers** from the EU. It will be required to have an "adequate" level of **data** protection to that of the EU so that personal **data transfers** from the EU to the UK can continue to take place. The government has confirmed that the UK will implement the GDPR.

EDGE, CIRU, UoS and GDPR

The security of data and especially the protection of personal data in the health setting in which we work, is of great importance. Since 2011 the CIRU has contracted a Tier 4 data hosting service which is accredited to host NHS N3 services. The CIRU has also maintained a successful submission and high compliance to the "Information Governance Toolkit" for a number of years. From April 2018 this accreditation will be submitted via the "Data Security and Protection (DSP Toolkit). The EDGE application is penetration tested annually for assurance of security against malicious breach attempts and unauthorised access.

The implementation of GDPR raises a number of questions about how data processors and data controllers will work together moving forward. Many of these are addressed through the amended Data Protection schedule that has been sent to all existing EDGE subscriber contracts, setting out the standard contractual clauses for processors. Responses to some of the changes can be found in the table below.

Regulations state: "The contract with the customer to include the following compulsory details…"		**Comments**
1	The Subject matter and duration of the processing	The subject matter, duration, nature and purpose of processing, the type of Personal Data, the categories of data subjects and the obligations of the controller are detailed in the Data Protection Schedule of EDGE contracts.
2	The nature and purpose of the processing	
3	The type of personal data and categories of data subject	
4	The obligations and rights of the controller	

Clinical Informatics Research Unit
NHSBT Southampton, MP852
Southampton General Hospital
Coxford Road, Southampton, SO16 5AF

t +44 (0) 2382 02 7200
e edge@soton.ac.uk
w www.edgeclinical.com
tw @EDGEclinical

Regulation states "The contract is to include the following compulsory terms…"		Comments
1	The processor must only act on the written instructions of the controller (unless required by law to act without such instructions)	Process Personal Data only on documented instructions from the controller is stipulated in the Data Protection Schedule for EDGE contracts
2	The processor must ensure that people processing the data are subject to a duty of confidence	Staff within the CIRU have already committed themselves to confidentiality through Information governance training provided by the University of Southampton, The Information Governance toolkit training and CIRU departmental spot checks and audits.
3	The processor must take appropriate measures to ensure the security of processing	Technical and organisational measures are already in place with Piksel-Carelink through accreditation through ISO 27001 and ISO 9001.
4	The processor must only engage a sub-processor with the prior consent of the data controller and a written contract	This is stipulated into the new Data Protection Schedule of EDGE contracts. CIRU do not envisage any further contracting with sub-processors beyond that with Piksel-Carelink.
5	The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR	This is written into the Data Protection Schedule of EDGE contracts.
6	The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notifications of personal data breaches and data protection impact assessments	This is written into the Data Protection Schedule of EDGE contracts. A subject access request form is available from the CIRU.
7	The processor must delete or return all personal data to the controller as requested at the end of the contract	This is already in our contracts
8	The processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state	This is written into the Data Protection Schedule of EDGE contracts.

Note: The new Data Protection Schedule of EDGE contracts reflects the current understanding of EU directive draft guidelines.

Clinical Informatics Research Unit
NHSBT Southampton, MP852
Southampton General Hospital
Coxford Road, Southampton, SO16 5AF

t +44 (0) 2382 02 7200
e edge@soton.ac.uk
w www.edgeclinical.com
tw @EDGEclinical

As a matter of good practice our contracts		Comments
1	state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR	This is written into the Data Protection Schedule of EDGE contracts.
2	reflect any indemnity that has been agreed	This is written into the Data Protection Schedule of EDGE contracts.
In addition to the article 28 .3 contractual obligations set out in the controller and processor contracts checklist , a processor has the following direct responsibilities under GDPR. The processor must		**Comments**
1	only act on the written instructions of the controller (Article 29)	CIRU (UoS) acceptance of these is noted in the updated (March 2018) Data Protection Schedule in the contract.
2	not use a sub-processor without the prior written authorisation of the controller (Article 28.2)	
3	cooperate with supervisory authorities (such as the ICO) in accordance with Article 31	
4	ensure the security of its processing in accordance with Article 32	
5	keep records of its processing activities in accordance with Article 30.2	
6	notify any personal data breaches to the controller in accordance with Article 33	
7	employ a data protection officer if required in accordance with Article 37	The University of Southampton employs a Data Protection Officer
8	appoint (in writing) a representative within the European Union if required in accordance with Article 27	Not required
A processor should also be aware that		**Comments**
1	it may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR	CIRU (UoS) is aware of the requirements of the GDPR and agrees to abide by the requirements of the European Economic area data protection law regarding the processing of personal data from the European Economic Area.
2	if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR	
3	if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR	
4	if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR	

Note: The new Data Protection Schedule of EDGE contracts reflects the current understanding of EU directive draft guidelines.

Clinical Informatics Research Unit
NHSBT Southampton, MP852
Southampton General Hospital
Coxford Road, Southampton, SO16 5AF

t +44 (0) 2382 02 7200
e edge@soton.ac.uk
w www.edgeclinical.com
tw @EDGEclinical

More Information

Additional information around the roles of data controllers and data processors, the introduction of GDPR, and roles and responsibilities of individuals and organisations can be found on the Information Commissioners website.

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

The NHS digital website will also be able to provide more specific guidance on GDPR within the NHS.

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

For guidance aimed specifically at researchers and study coordinators managing individual research projects the HRA have produced specific guidance.

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/

Your organisations will have been preparing for GDPR since its announcement in 2017. Your local Information Governance team will be able to provide you with additional guidance about your organisations GDPR implementation plan.

Alternatively, you can contact our team direct on edge@soton.ac.uk

Clinical Informatics Research Unit
NHSBT Southampton, MP852
Southampton General Hospital
Coxford Road, Southampton, SO16 5AF

t +44 (0) 2382 02 7200
e edge@soton.ac.uk
w www.edgeclinical.com
tw @EDGEclinical