Statement of General Data Protection Regulation (GDPR) Compliance

Duke University and Duke University Health System (DUHS)

What is the GDPR?

Effective May 25, 2018, the European Union (EU) passed the European Union General Data Protection Regulation (EU GDPR) a data privacy regulation that, generally speaking, is applicable throughout the European Economic Area (EEA), and to those who collect personal data about people in the EEA. The GDPR formally codifies privacy as a fundamental right.

Duke's Response to the GDPR

A GDPR Coordination Group led by Duke's Privacy Officer, was developed with membership made up of key University and DUHS leaders from Compliance and Privacy, Counsel, Information Security, Information Technology, Purchasing, and Research Administration.

A GDPR Data and Project sub-Group made up of key University and DUHS leaders from Counsel, Corporate Risk Management, Global Support, Information Technology, Research Administration, and Student Affairs provided additional input and support to the Coordination Group. In addition, Duke engaged the services of outside counsel for expert guidance regarding its GDPR implementation plan

The GDPR Coordination Group developed and communicated Duke's approach to GDPR with deliverables to key stakeholders including:

- Duke University Privacy Statement (https://oarc.duke.edu/privacy/duke-university-privacy-statement)
- Duke University Privacy Policy (link found within the Duke University Privacy Statement)
- GDPR in-person training for identified priority areas
- Creation of GDPR Data Subject Privacy Rights Request Form; development of process for handling receipt of rights requests
- Creation of GDPR@duke.edu email account for receipt of rights requests and all other GDPR inquiries
- Implementation of cookie bar for Duke websites
- Development of GDPR Article 30 Records of Processes

Statement of Duke University's Lawful Basis for Collecting or Processing Personal Data.

Under the GDPR, Duke University will often have a lawful basis to collect and process Personal Data, including without limit, under one or more of the following categories:

a) Processing is necessary for the purposes of the legitimate interests pursued by Duke University or by a third party.
b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
c) Processing is necessary for compliance with a legal obligation to which Duke University is subject.

d) The Data Subject has given consent to the processing of their Personal Data for one or more specific purposes.

Statement of Duke University Data Protection Standards

Duke information security policies and procedures are aligned, where applicable, with the US National Institute of Standards and Technology ("NIST") CyberSecurity Framework ("CSF") and the CI Security Critical Controls, as well as the US Health Insurance Portability and Accountability Act ("HIPAA") and is guided by our risk-based approach to securing resources and data..

Areas addressed by policies and procedures include, but are not limited to:

- Identity and Access Management
- Data Loss Prevention
- Encryption & Pseudonymization
- Incident Response Plan
- Third-Party Risk Management
- Policy Management

Contact Us

If you have any questions, comments, requests or concerns about this Statement of Compliance, Duke's GDPR implementation plan, or other privacy-related matters, you may contact us in the following ways:

Email: GDPR@duke.edu

Phone: 919-684-2144

Address: Duke Privacy
Office of Audit, Risk & Compliance
Box 90436
705 Broad Street, Suite 210
Durham, NC 27708

Data Protection Officer: Keith E. Stouder, Information Technology (IT) Risk and Privacy Officer

You may also direct GDPR inquiries to Duke University's Article 27 Representative:

Irene Lau, Executive Assistant
Duke Corporate Education Limited
165 Fleet Street
London EC4A2DY
United Kingdom