Statement of General Data Protection Regulation (GDPR) Compliance

Duke University and Duke University Health System (collectively, "Duke")

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 individuals in the EEA. Individual rights established by the GDPR with respect to personal data include the right to be informed about collection and use, the right to access, the right to be forgotten, and the right to restrict processing.

While Duke has students, staff, patients, collaborators, and visitors who are citizens and residents of, or may be located in, countries in the EEA, only certain activities conducted by Duke may give rise to obligations under GDPR. Those areas at Duke most likely to intersect with GDPR obligations include programs or other activities conducted by Duke throughout the EEA and the collection of personal information of, and marketing or development targeted to, individuals in the EEA.

Duke's Response to the GDPR

A GDPR Coordination Group led by Duke's Privacy Office, 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 engages the services of outside counsel for expert guidance.

Duke's approach to GDPR includes:

- Key provisions included in the Duke University Privacy Statement (https://oarc.duke.edu/privacy/duke-university-privacy-statement)
- Training and resources
- GDPR Data Subject Privacy Rights Request Form and process for handling receipt of rights requests
- privacy@duke.edu email account for receipt of rights requests and all other GDPR-related inquiries
- Privacy cookie bar for Duke websites
- GDPR Article 30 Records of Processing Activities

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

As set forth in greater detail in its Privacy Statement, Duke 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 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 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 Data Protection Standards

Duke information security policies and procedures are aligned, where applicable, with the U.S. National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF") and the Center for Internet Security ("CIS") Critical Security Controls, as well as the U.S. 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
- Data Classification Standard

Contact Us

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

Email: privacy@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: Leigh P. Goller, Chief Audit, Risk and Compliance Officer

You may also contact Duke's Article 27 Representative, an individual who has been designated by Duke to communicate with data subjects regarding GDPR matters:

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