



Änderung datenschutzrechtlicher Bestimmungen durch die Datenschutz-Grundverordnung (DSGVO)

Informationen für Beschäftigte der Humboldt Universität zu Berlin (HU) zur Umsetzung der neuen EU-Datenschutz-Grundverordnung

Ab dem 25. Mai 2018 gilt die neue Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), kurz DSGVO. Sie entwickelt den Datenschutz fort. Viele Regelungen orientieren sich am bisherigen deutschen Datenschutzrecht. Einige neue Regelungen werden hinzukommen. Die DSGVO stützt sich auf die bewährten Grundprinzipien des Datenschutzes. So bedarf jede Verarbeitung personenbezogener Daten auch künftig einer Rechtfertigung durch eine rechtliche Grundlage oder durch die Einwilligung der Betroffenen. Die Prinzipien der Datenminimierung (Datenvermeidung/Datensparsamkeit), der Erforderlichkeit, der Zweckbindung und der Transparenz bleiben erhalten. Die DSGVO bringt allerdings umfassende Nachweispflichten mit sich. Die Verantwortlichen müssen nicht nur sicherstellen, dass sie die Vorgaben der DSGVO erfüllen, sondern dies zudem auch nachweisen können, vgl. Art. 5 Abs. 2 DSGVO (sog. „Rechenschaftspflicht“/„accountability“).

Da eine vollumfängliche Darstellung der Änderungen in dieser kurzen Übersicht nicht möglich ist, sollen im Folgenden nur die wichtigsten für den Universitätsbetrieb der HU relevanten Neuregelungen vorgestellt werden.

1. Ab wann gilt die DSGVO und was sind die Auswirkungen?

Die DSGVO ist zwar schon am 24. Mai 2016 in Kraft getreten, gilt aber erst ab dem 25. Mai 2018 und verdrängt die alten nationalen Datenschutznormen. Sie wird dann unmittelbar und gegenüber bestehenden nationalen Gesetzen vorrangig angewendet. Allerdings enthält die DSGVO in einigen Fällen sog. Öffnungsklauseln und bietet dem nationalen Gesetzgeber Raum für eigene Regelungen, welche spezifische Sachverhalte konkreter regeln sollen. Das bedeutet, dass sich datenschutzrechtliche Regelungen zwar vorrangig aus der DSGVO ergeben werden; es wird jedoch auch noch weitere nationale Regelungen geben. Aufgrund der weitreichenden Spielräume durch die Öffnungsklauseln, insbesondere den öffentlichen Bereich betreffend, wie etwa in Art. 6 Abs. 2 und 3, Art. 9 Abs. 4 und Art. 23 DSGVO, dürften auch bisherige Regelungen zum überwiegenden Teil erhalten bleiben.

2. Die wichtigsten Handlungsziele im Überblick

a) Aktualisierung der Rechtsgrundlagen und Einwilligungen

Es können sich mit der DSGVO die Normen der Rechtsgrundlagen der Datenverarbeitung ändern, welche gegebenenfalls anzupassen sind. Eventuell sind auch Einwilligungen zur Datenverarbeitung erneut einzuholen, sofern diese nicht mit Art. 4 Nr. 11, Art. 7 f. DSGVO übereinstimmen.

b) Anpassung von Informationstexten zu Datenverarbeitungen

Die DSGVO legt den Verantwortlichen weitreichende Informationspflichten gegenüber den Betroffenen auf, Art. 12 DSGVO. Gegebenenfalls sind die Texte zur datenschutzrechtlichen Information der Betroffenen bei Datenverarbeitungen an die in Art. 13 und 14 DSGVO

aufgelisteten Vorgaben anzupassen, sofern die notwendigen Angaben nicht schon vorgenommen wurden.

c) Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO

Für Datenverarbeitungen mit hohem Risiko für die Rechte der Betroffenen ist eine Abschätzung der Risiken und möglichen Folgen vorzunehmen. Aufgrund von Art. 35 Abs. 7 lit. d DSGVO wird den Verantwortlichen empfohlen, grundsätzlich eine Datenschutz-Folgenabschätzung vorzunehmen, um den Nachweispflichten (Art. 5 Abs. 2 DSGVO) nachzukommen. Die Datenschutz-Folgenabschätzung muss mindestens die in Art. 35 Abs. 7 lit. a-d geforderten Angaben enthalten. Hierzu gehören neben der systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke auch eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen einschließlich der zur Bewältigung der Risiken geplanten Abwehrmaßnahmen. Zudem ist eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck vorzunehmen.

d) Verzeichnis von Verarbeitungstätigkeiten

Die neue DSGVO verpflichtet zu umfangreichere Dokumentation. Nach Art. 30 Abs. 1 DSGVO ist von den Verantwortlichen ein schriftliches Verzeichnis von Verarbeitungstätigkeiten anzufertigen. Nach Art. 30 Abs. 1 lit. a-g müssen auch weiterhin die wesentlichen Angaben wie Kontaktdaten, Datenkategorien, Verarbeitungszwecke, Kreis der betroffenen Personen und Datenempfänger angegeben werden. Jedoch müssen nunmehr nach Art. 30 Abs. 2 DSGVO auch die Auftragsverarbeiter, also die externen, zur Datenverarbeitung beauftragten Stellen, ein Verzeichnis von Verarbeitungstätigkeiten führen.

e) Neuformulierung der Auftragsdatenverarbeitungsverträge

Aufgrund der neu eingeführten Verzeichnisführungspflicht auch der Auftragsverarbeiter nach Art. 30 Abs. 2 DSGVO sind auch die Auftragsdatenverarbeitungsverträge neu zu formulieren. Die hierzu notwendigen Angaben sind in Art. 30 Abs. 2 lit. a-d DSGVO aufgelistet.

f) Betroffenenrechte

Die DSGVO stärkt die Betroffenenrechte und regelt diese umfassender (Art. 12-23 DSGVO). So wird z.B. das Recht auf Datenübertragbarkeit (Art. 20 DSGVO) eingeführt und das Recht auf „Vergessenwerden“ erstmals ausdrücklich benannt (Art. 17 DSGVO). Kernstück sind Transparenz und Information der Betroffenen.

g) Rechenschaftspflicht

Nach Art. 5 Abs. 2 DSGVO hat der Verantwortliche die Einhaltung der bereits bekannten datenschutzrechtlichen Grundsätze aus Art. 5 Abs. 1 DSGVO sicherzustellen, wie beispielsweise Transparenz, Zweckbindung, Datensparsamkeit oder angemessene Sicherheit der Datenverarbeitung. Nunmehr muss der Verantwortliche hierfür im Zweifel Nachweise erbringen können. Er trägt also eine Rechenschaftspflicht über die Einhaltung datenschutzrechtlicher Grundsätze. Mithin sollte ein dokumentiertes Datenschutzkonzept angestrebt werden.

h) Meldepflichten gemäß Art. 33, 34 DSGVO

Verletzungen des Schutzes personenbezogener Daten sind unverzüglich und möglichst binnen 72 Stunden der Aufsichtsbehörde und der betroffenen Person mitzuteilen.