netdocuments®

Quick Facts

NetDocuments and the GDPR

Important Things to Know

What is the GDPR? The General Data Protection Regulation (GDPR) is a law enacted by the European Union (EU) which protects the rights of natural persons in the EU and the European Economic Area (EEA) regarding how their personal data is processed and how their personal data moves inside and outside the EU.

What does the GDPR regulate? The GDPR regulates entities inside or outside the EU which process the personal data of persons in the EU. The regulation also specifically addresses international transfers of personal data. Terms which are points of focus in the regulation include:

PERSONAL DATA

"means any information relating to an identified or identifiable natural person ('data subject')" which can identify, directly or indirectly, the data subject.
Article 4(1)

PROCESSING

NetDocuments is a Processor.

"means any operation… performed on personal data… such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."
Article 4(2)

CONTROLLER

A customer of Netdocuments is a Controller.

"means the natural or legal person, public authority, agency or other body which… determines the purposes and means of the processing of personal data."
Article 4(7)

PROCESSOR

"means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."
Article 4(8)

Under these definitions, law firms and other organizations which use the NetDocuments Service are controllers and NetDocuments is a processor. The NetDocuments Document Management Service (DMS or "Service") processes documents for controllers and some or many of those documents may contain personal data.

For transfers of personal data to third countries the GDPR states that "any transfer of personal data which are undergoing processing or are intended for processing… shall take place only if… the conditions laid down in this [regulation] are complied with by the controller and processor…."

Who must comply? The GDPR applies to entities inside and outside the EU that process the personal data of persons in the EU. The regulation also controls the transfer of such data to entities or locations outside of the EU.

Why comply? The GDPR imposes fines of up to €20,000,000 (approximately $23,600,000) or up to 4% of the world-wide revenue of an entity's preceding financial year, whichever is higher, for violations of its regulations.

What is the GDPR timeline?

Passed on 27 April 2016, the GDPR replaces the EU Data Protection Directive or DPD.

On 12 July 2016, the EU Commission issued an Adequacy Decision stating that the United States ensures an adequate level of protection for transferring personal data between the EU and US under the EU-US Privacy Shield Framework.

GDPR enforcement begins 25 May 2018.

> "NetDocuments recognizes the GDPR sets a new and higher bar for personal data protection, security, and compliance. While your journey to GDPR compliance can seem challenging, NetDocuments is here to help our global customers."
>
> —Alvin Tedjamulia,
> Chief Technology Officer

Specific GDPR Requirements

The regulation identifies six principles for how personal data shall be processed, guarantees eleven rights of data subjects, requires implementation of identified security measures, and regulates data transfers to third counties. Controllers must follow these requirements to adequately protect personal data.

Principles for Processing Personal Data

1. Processed lawfully, fairly, and in a transparent manner. **Article 5(a)**
2. Collected for specified, explicit, and legitimate purposes. **Article 5(b)**
3. Adequate, relevant, and limited to what is necessary. **Article 5(c)**
4. Accurate and kept up to date. **Article 5(d)**
5. Kept no longer than necessary. **Article 5(e)**
6. Kept Securely. **Article 5(f)**

Rights of Data Subjects

1. The right to clear and plain language, and accessible modalities of communication. **Article 12**
2. The right to timely disclosure of processing and contact details where personal data are collected from the data subject. **Article 13**
3. The right to timely disclosure of processing and contact details where personal data has not been obtained from the data subject. **Article 14**
4. The right of access by the data subject. **Article 15**
5. The right to rectification. **Article 16**
6. The right to erasure ('right to be forgotten'). **Article 17**
7. The right to the restriction of processing. **Article 18**
8. The right of notification regarding rectification or erasure or restriction. **Article 19**
9. The right to data portability. **Article 20**
10. The right to object. **Article 21**
11. The right to refuse automated decision-making, including profiling. **Article 22**

Required Security Measures

Systems and operations used to process personal data must be designed to be secure in operation and to provide core security as a default function **(protection "by design and by default" Article 25)**. Controllers and processors have specific security requirements **(Articles 24, 28)**. Controllers must maintain records of their processing activities **(Article 30)**, and specifically implement "appropriate technical and organizational measures" to ensure appropriate security, including encryption, confidentiality, availability, restoration, regular testing and evaluation, and consideration of potential risks **(Article 32).**

Securely Transferring Data to Third Countries

Transfers to countries outside of the EU shall only take place if one of the following provisions is met:

An Adequacy Decision **Article 45**
The EU Commission has made an adequacy decision that the destination country ensures adequate protection of personal data; or

Appropriate Safeguards **Article 46**
The controller or processor has put in place one of the following appropriate safeguards:

a. A legally binding and enforceable instrument between public authorities;

b. Binding corporate rules approved by a competent supervisory authority;

c. Standard data protection clauses adopted by the Commission;

d. Standard data protection clauses adopted by a supervisory authority and approved by the Commission;

e. An approved code of conduct together with binding and enforceable commitments from the controller or processor; or

f. An approved certification mechanism, together with binding and enforceable commitments from the controller or processor.

How NetDocuments (a Processor) Complies with the GDPR

NetDocuments meets the GDPR security requirements for processors **(Article 28)** through the company's implementation of a comprehensive security infrastructure. The company securely transfers data to third countries under an Adequacy Decision for the US-EU Privacy Shield agreement, and as other Appropriate Safeguards become available, NetDocuments will implement those which provide the most value and protection to NetDocuments and its customers.

How NetDocuments Helps its Customers (Controllers) comply with the GDPR

The NetDocuments Service is designed and operated so that all customer (controller) documents stored in the Service, including documents which may contain personal data, are kept private and secure, both at rest and in transit. NetDocuments personnel have no knowledge as to the type or contents of customer (controller) documents. Because of this, some of the principles for processing personal data and protecting the rights of data subjects are not directly applicable to NetDocuments. Instead, NetDocuments becomes a primary service enabling controllers to comply with many core GDPR requirements. Examples include:

Processing Standards. NetDocuments provides tools and functions that directly assist controllers in securely complying with many controller-side requirements.

NetDocuments enables customers to accurately control how long to retain documents, how to manage documents, and how to store and transmit documents securely. **Articles 5, 6, 7**

Rights of Data Subjects. NetDocuments provides a secure and convenient way for controllers to honor and maintain data subject rights. NetDocuments' tools and functions help customers keep track of how they gather data subject information, where to store, and what personal data to gather and not gather. **Articles 5-21**

Rectification of Data Subjects. NetDocuments simplifies finding personal data for responding to rectification requests and provides controls to erase documents as required. NetDocuments maintains all customer documents in their original format to ease document portability. **Articles 12-21**

Identifying Personal Data in Images. Users can quickly organize image files by type and subject. Popular third-party OCR applications easily integrate into the Service to scan and identify personal data in the images, and NetDocuments is actively developing additional, integrated OCR solutions for expected availability in 2018. **Articles 12-14**

Records of Processing Activities. NetDocuments includes reporting and documentation features to facilitate customers meeting GDPR Article 30 requirements for maintaining records of processing activities, including purposes of processing, categories of data subjects, records of document transfers, retention schedules, and processes for protecting and erasing documents. **Article 30**

Standard International Transfers. NetDocuments complies with GDPR adequacy decisions for secure and legal transfer of personal data to the US. NetDocuments plans to comply with future GDPR transfer requirements as they are adopted or made available. **Articles 44-47**

Multi-office Support. NetDocuments is a highly-secure, legally-compliant application that customers can deploy across multiple customer offices located in different countries inside and outside of the EU for centrally managing documents that may contain personal data. **Articles 44-47**

The table at the end of this document lists key actionable articles in the GDPR, identifies the regulated activity in each article, and states the level of responsibility for NetDocuments' customers (Controllers) and for NetDocuments (a Processor). A separate white paper from NetDocuments details the actions and responsibilities for each article.

GDPR Article	Regulated Activity	Customer Responsible	NetDocuments (Processor) Responsible
3(2)(a)	Offering goods & services to data subject	Yes	Support
3(2)(b)	Monitoring data subject behavior within EU	Yes	No
3(3)	Processing by Controllers outside EU	Yes	Yes
5(1)(a), 6	Lawful, fair, & transparent processing	Yes	Yes
5(1)(b)	Data collection purpose limitation	Yes	Support
5(1)(b)	Data archiving purpose limitation	Yes	Yes
5(1)(c)	Personal data minimization	Yes	No
5(1)(d)	Personal data accuracy	Yes	Support
5(1)(e)	Personal data storage period limitation	Yes	Support
5(1)(e)	Personal data archiving safeguards	Yes	Support
5(1)(f)	Processing integrity & confidentiality	Yes	Yes
5(2)	Accountability for compliance with GDPR	Yes	Yes
7(1)	Obtaining & demonstrating consent	Yes	No
7(2)	Consent uses clear & plain language	Yes	No
7(3)	Easy for data subject to withdraw consent	Yes	Support
7(4)	Requiring consent when not necessary	Yes	No
8(1)	Obtaining parental consent for children	Yes	No
8(2)	Verifying validity of parental consent	Yes	No
9(1) & (2)	Revealing special categories of personal data	Yes	Yes
9(1) & (2)	Uniquely identifying persons or special data	Yes	Yes
10	Processing criminal conviction data	Yes	Support
12(1)	SAR responses in clear & plain language	Yes	No
12(2)	Facilitating SARs & auto-profiling opt out	Yes	Support
12(3) & (4)	SAR responses without undue delay	Yes	No
12(3)	SAR responses by electronic means	Yes	Support
12(5)	Charging for SAR responses	Yes	No
12(6)	Requesting additional info for SAR responses	Yes	No
12(7) & (8)	Providing icons in SAR responses	Yes	No
13(1) & (2)	SAR response details (direct collection)	Yes	Support
13(3) &14(4)	Disclosure of further processing details	Yes	Support
14(1) & (2)	SAR response details (indirect collection)	Yes	Support
14(3)	SAR response (indirect collection) time limits	Yes	No
15(1)	Right of access to personal data	Yes	Support
15(2)	Right of being informed of third country transfer	Yes	Support
16	Right to rectification (correction of inaccuracies)	Yes	Support
17	Right to erasure ('right to be forgotten')	Yes	Support
18	Right to restriction of processing	Yes	Support
19	Right to notification about rectification or erasure	Yes	Support
20	Right to data portability	Yes	Support
21	Right to object to processing	Yes	Support
22	Right to not be subject to automated processing	Yes	No
25(1)	Data protection by design	Yes	Yes
25(2)	Data protection by default	Yes	Yes
28(1)	Processor technical/organizational measures	Selection	Yes
30	Records of processing activities	Yes	Yes
31	Cooperating with supervisory authority	Yes	Yes
32(1)(a)	Security of processing (encryption)	Selection	Yes
32(1)(b)	Security of processing (ensuring CIA & R)	Selection	Yes
32(1)(c)	Security of processing (can restore/recover)	Selection	Yes
32(1)(d)	Security of processing (reviews & audits)	Selection	Yes
32(2)	Security of processing (risk assessments)	Selection	Yes
32(4)	Process only on instruction from controller	Yes	Yes
33	Notification of data breach to authority	Yes	Support
34	Notification of data breach to data subject	Yes	Support
35	Data Protection Impact Assessment	Yes	Yes
36	Consulting with authorities prior to processing	Yes	Support
37	Designate a Data Protection Officer	Yes	Yes
45, 46	Secure transfers to third countries	Yes	Yes

Note: This table lists key actionable articles in the GDPR, identifies the regulated activity in the article, and illustrates the level of responsibility controllers and NetDocuments (a processor) have for the listed activity.

NetDocuments is Your Best Path to GDPR Compliance

NetDocuments provides a superior document and email management solution for centrally securing and managing your documents and emails, for protecting personal data, for legally enabling document transfers between the US and the EU, and for helping your entity comply with the GDPR. No other products on the market today offer all of the features found in NetDocuments, including:

Global Document and Email Management

Comprehensive Functionality helping Customers (Controllers) Meet GDPR Compliance Requirements

Security by Design and Default with multi-layered document encryption, including customer-managed encryption keys

Highest-in-industry User Adoption

Industry leading Ease-of-Deployment and Ease-of-Use

netdocuments®

For more information about the NetDocuments DMS, please visit netdocuments.com or contact a NetDocuments representative.

Legend

Yes

Direct responsiblity for the requirements

Selection

The entity chooses how it meets the responsibility

Support

The entity enables compliance with the responsibility

No

Entity does not have responsibility for the requirement.

*SAR is Subject Access Request.