



Product Fact Sheet - GDPR Capabilities

Product Name Case Management & Knowledge Portal

Description of the product HR Electronic Signature in Partnership with DocuSign®

HR processes supported

Sign online all types of contracts, endorsements, annual interviews, etc.

- Automate signatures for large volumes of documents
- Get double signatory authentication by email and SMS
- Automatically or automatically restart pending signatures
- Adapt notifications to each type of signatory

Categories of personal data supported

To be customized by each Customer, categories of personal data may include:

- Personal identification data (name, title, private address, phone numbers ...);
- Electronic identification data (IP addresses, cookies, connection times);
- Personal details (age, sex, date of birth, place of birth, marital status and nationality); and
- Signed documents

GDPR Aspect	Article	Understand how to comply using PeopleDoc
Data Controller	Article 4 (7) Article 24	Customers
Data Processor	Article 4 (8) Article 28	PeopleDoc
Transparency	Article 5, §1 (a)	PeopleDoc's Services Privacy Policy is easily accessible through the platform
Access to data	Article 15	All data hosted in PeopleDoc Services is available for reporting. Customers can define their own policies to extract data. PeopleDoc will cooperate with Customers in answering access requests received directly by PeopleDoc
Rectification and erasure	Articles 16 & 17	Customers' users with appropriate permissions can change an individual's personal data, delete documents and/or establish pre-defined data retention rules
Restriction of processing	Article 18	Role-based permissions allow customers to define which users or roles can display, edit, or delete data. It is also possible to restrict access to historical data to specific roles
Data portability	Article 20	Most data hosted in PeopleDoc Services is available for reporting and download Customers may choose to use the Reversibility procedure and/or delete data at the end of the service provision
Privacy by design and by default	Article 25	PeopleDoc Services aim to be designed to support all technical data protection requirements; however, customers are still responsible for configuring and using them accordingly. PeopleDoc Services meet the privacy by default requirements if customers configure, for example, data retention, data minimization and relevant security safeguards accordingly
Sub-Processing	Article 28, §4	All information regarding PeopleDoc's sub-processors can be found on: https://www.people-doc.com/legal/sub-processors
Data Security	Article 32	ISO/IEC 27001:2013 and SOC 2 Type 2 Report
Data breach notification	Article 33	In the event PeopleDoc becomes aware of any unauthorized access to or disclosure of Personal Data, PeopleDoc will promptly notify affected Customers, according to its <i>Incident Management Policy</i> and <i>Personal Data Breach Response Policy</i>
Data protection impact assessment	Article 35	PeopleDoc assists Customers in ensuring compliance with its obligations
Data Protection Officer	Article 37	PeopleDoc's Data Protection Officer can be reached at privacy@people-doc.com
Cross-border transfer	Articles 45 to 50	Customers can choose to host data in either the US or the EU platform. PeopleDoc ensures complete independence between the two hosting areas