# FileFacets for GDPR

## Solution Overview for Compliance

# Contents

# FileFacets Overview

FileFacets Enterprise ID is an online privacy compliance and enterprise analytics platform that makes it easy for businesses to locate and process unstructured content from multiple sources across the enterprise to protect sensitive data and mitigate risk.

The all-in-one platform enables organizations to perform sophisticated data discovery and advanced content search of networks, servers, desktops and laptops - identifying to protect sensitive corporate information and personal data, removing Redundant, Obsolete and Trivial data (ROT), and facilitating the secure transfer of data between repositories.

**SaaS and Secure**

FileFacets is a Software-as-a-Service (SaaS) platform, meaning all project work takes place within the online platform. FileFacets runs on the Microsoft Azure Cloud in SOC2 / SSAE16 secured datacenters around the world.

FileFacets platform establishes a secure the connection to the client's environment via the FileFacets Software Agent, providing a single point of connectivity through an organization's firewall where it can access each system within an organization. It is important to note that only the metadata (file properties) are communicated to the cloud. All scans and scan results are stored locally and all source files remain unaltered and unmoved.

**FileFacets for GDPR Data Subject Rights**

FileFacets provides the platform and methodology to help businesses comply with the EU's GDPR. With years of experience in information governance, FileFacets provides the tools for acquiring data, and identifying and actioning of personal data from multiple sources.

Through a sophisticated, yet simple interface, FileFacets allows businesses to scan multiple unstructured data sources and repositories (networked and cloud-based shared drives, servers, enterprise content management systems, email, desktops, and laptops) to locate and identify any personal data or sensitive data an organization may possess.

FileFacets will monitor for any new content being created that contains personal data so that it can be identified, flagged, moved, deleted or secured in a safe environment.

# GDPR Key Changes

The General Data Protection Regulation (GDPR) was designed to harmonize data privacy laws across Europe. It emphasizes transparency, security and accountability by businesses and aims to standardize and strengthen the right of European citizens to data privacy. It replaces the existing data protection framework under the EU Data Protection Directive (DPD).

The GDPR is a holistic approach to data protection that requires businesses to adopt processes and procedures on the collection of data, and the storage and lifecycle management of the personal data of its customers, contacts and employees. And it's having a global impact - reshaping the way organizations across the world approach data privacy.

Many of the main concepts and principles of GDPR are much the same as those found in the current Data Protection Acts 1988 and 2003, so if a business is compliant under current law, then much of their approach should remain valid under the GDPR.

However, GDPR introduces new elements and significant enhancements, which will require detailed consideration by all organizations involved in processing personal data. Some elements of GDPR will be more relevant to certain organizations than others, and it is important (and useful) to identify and map out those areas that will have the greatest impact on your business model.

A full version of the GDPR Regulations can be found at: https://gdpr-info.eu/

## Key Changes to Policy

**Expanded Territory**

The GDPR does away with the criterion of number of employees and focuses instead on what organizations do with personal information. Any company, regardless of location, that processes the personal data of an EU resident is subject to the GDPR. Any non-EU businesses that process the data of EU citizens must appoint a representative in the EU.

**Penalties**

Fines for non-compliance of the new GDPR regulations are significant. Businesses can be fined from 2% of global revenue for not having their files in order (Article 28) up to 4% of annual global revenue or €20 million (whichever is greater) for breaching the GDPR.

**Consent**

When an individual provides consent for the use of their data, consent must be easy to understand, and it must be just as easy to withdraw consent as it was to give it. Why the data is being collected, and for what purpose(s) must be conveyed in a concise form, in laymen's terms – no legalese.

**Privacy by Design**

The GDPR calls for the inclusion of data protection from the onset of the designing of systems and processes, rather than just as an addition. Businesses need to develop processes that outline what information, and for what use personal data is being retained - and how the data is being collected, where the data is located, and for how long the data will be stored. Data Controllers must hold and process only the data absolutely necessary for the completion of duties, as well as limit access to personal data only to those necessary for processing. Some businesses may need to appoint a Data Protection Officer (DPO).

## Key Changes to Data Subject Rights

**Right to Access**

Individuals can get confirmation of what personal information is being processed, where it is being stored, and why their information is being held. If EU citizens wish to know, a Controller must provide electronic copies of this data to the individual, free of charge.

**Right to be Forgotten**

Individuals are entitled to have their data erased, ceased from further dissemination, and potentially have third parties halt processing of data. In the case that their data is no longer relevant to why they originally gave their information, they may also have their data erased.

**Right to Data Portability**

The right to data portability allows individuals to obtain and reuse their data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way.

**Right to Notification**

In the event of a data breach, businesses are required to notify their Data Protection Authority (DPA) within 72 hours of the breach. Individuals are also entitled to be notified in the event of a breach of their personal data.

# FileFacets for GDPR

FileFacets can be used in a number of ways to solve for data protection and information management requirements, from planning through to execution, of a businesses' GDPR strategy:

**Data Discovery & Data Protection**

FileFacets can be used for data discovery and content analytics for a businesses' Data Protection Impact Assessment (DPIA) to:

- Identify documents that contain personal data in each repository.
- Identify document types and categories that are likely to contain sensitive or personal data.
- Define automated data processing rules to mitigate risk.
- FileFacets can be used for on-going reporting on personal data across the enterprise, identifying what files contain personal data, and where they reside.

**Risk Mitigation**

FileFacets can be used for risk mitigation by establishing processes and procedures for the handling of files that contain personal data by:

- Applying file classifications and attributions to sensitive files.
- Automating business processes for sensitive data handling.
- Migrating or auto-archiving sensitive documents to a secure location.

**Reporting**

For reporting requirements for internal governance, or the external Data Protection Authority (DPA), FileFacets can:

- Identify all files across multiple repositories, email, and desktops in an organization.
- Identify all documents and records containing personal data that may have been affected in the event of a data breach.
- Produce a comprehensive list of records that contain personal data, by repository, by subject, etc.
- Export or copy files that were affected by a breach.
- Audit users' decisions on the requests and actions of files and file types.

**Data Subject Rights**

For the regulations' directive for transparency, FileFacets can easily locate, produce, and action certain files containing personal data to meet the requirements for:

- *Right to Access:* where an individual requests to view and retain a copy of all of their personal data being held by an organization
- *Right to Data Portability:* where an individual requests to retain a copy to move their personal data records to another business or service provider
- *Right to be Forgotten:* where an individual requests to have their personal data removed from a business' data stores
- *Right to Notification:* reporting on compromised data in the case of a breach of an individual's personal data

**Information Governance**

For ongoing data maintenance of repositories, FileFacets can assist in implementing best practices in information management (IM) and information governance (IG) including the:

- Rationalizing, organizing, and the enabling of Enterprise Content Management (ECM) best practices.
- Classification, attribution, and organization of content across multiple repositories
- ROT processing (purging of Redundant Obsolete and Trivial data), content classification, taxonomy implementation, metadata attribution, and multi-repository migration.

## FileFacets Methodology for GDPR Data Processing

FileFacets' process for GDPR readiness is a series of data analytics, advanced searches and business processes that ensure users:

- Understand what data they have.
- Identify personal data in their data stores.
- Put business processes in place to best protect sensitive data.
- Have the ability to retrieve records that contain personal data should a request be made.

FileFacets does this through the following methodology:

1) **Content Analytics:** delivers a single enterprise-wide view of all content across multiple repositories
2) **File Clean-Up:** eliminates all files that are Redundant, Obsolete, and Trivial (ROT) in data stores
3) **Upload Search Text:** upload customer and contact lists to search for personal data
4) **Find & Flag:** perform searches on all data stores to locate and flag files that contain personal data
5) **Define Actions:** define actions or business processes for each type of personal data
6) **Monitor:** set up scheduled scans to search for new content and content changes

**Content Analytics**

The first step in understanding what personal data an organization holds is to understand exactly how much data they are dealing with: *how many* files a business has, *where* they are, and *what* they are. FileFacets Content Analytics Dashboard gives businesses a unified view of all their content to better understand and analyze what data exists, and where across the entire organization.

FileFacets performs two types of scans:
*Initial scan:* The initial scan scans the file properties to identify the number of files across multiple systems, identifies duplicates and Redundant, Obsolete, Trivial (ROT) data as well as type, size, and age of files.
*Full Scan:* The full scan scans the full text index of the files to identify files that contain personal data, specific search terms and to perform file clustering, grouping data by document type and content.

FileFacets scans all content across multiple repositories and displays the content analysis into a single enterprise-wide view. Next, through advanced searching and machine-learning clustering it identifies which files are similar in nature, and can also identify which files contain personal data.

Scan results are stored locally, behind the enterprise firewall, ensuring any sensitive data is not transferred to the cloud.

**File Clean-Up**

Most file repositories contain a large number of files without any valid business value. Redundant, Obsolete, and Trivial records (otherwise known as ROT) are those files that clutter your records repository and cause file systems and Enterprise Management Systems (ECMs) to become increasingly difficult to manage. These may be duplicates, out of scope content, or files deemed as otherwise trivial. Removing these files from a business' data stores reduces an organization's data set to only those records that contain business value reducing storage costs, back up time, and minimizing the risk of outdated personal data being compromised or missed.

***Redundant Files***

Files are analyzed for duplication by MD5 hash analysis. Files with the exact same content, regardless of the file names or dates, are marked as duplicates. A simple rule such as "keep oldest", or "keep newest" can then be applied to determine which file of a duplicate stays, and which one goes. Redundant files can be moved to a common folder, for deletion or archiving.

***Obsolete Files***

There are two ways the FileFacets platform cleans up obsolete or outdated files. The first is to assign a date threshold to files. This could be defined as files that have not been accessed in 12 months, or created by a user who has not created new content in 24 months. This flags older files for movement to an "Outdated" folder when records are moved. This is a quick way to clean up obviously outdated files. The second, and more extensive approach, involves the classification of files to your organization's retention schedules. This approach is fully supported within FileFacets.

***Trivial Files***

Trivial files are files that do not have any ongoing business value. Analysis of trivial content is accomplished quickly while further reducing information holdings. Using FileFacets, files can be identified as trivial by file type, file size or age. File extensions that are no longer supported or file types that are associated with personal information (such as mp3's) or system files (such as .tmp, .db, .dll files) can be quickly identified and queued for removal. Analyzing files by file size highlights files which are either too small to contain content, or too large to be stored in the current location. FileFacets can report on all files by their age and users can determine business rules to quickly segregate them for archive or removal.

**Upload Search Text**

Uploading custom search lists allows businesses to search for and identify all files that contain the personal data for specific individuals. Users can define individual's data points by uploading search variables in an Excel or .csv list into FileFacets, for example a customer list or an employee list, containing the personal data of each data subject. Each individual becomes its own search term, with a group of keywords or phrases that FileFacets will search against to retrieve the files that contain the personal data within the organization's multiple systems.

Custom search data is stored locally, behind the enterprise firewall, ensuring no sensitive personal data is transferred to the cloud.

**Find & Flag**

FileFacets performs advanced content searching that finds and identifies content in two ways:
*Pattern Search:* which allows users to search for and locate files that contain a specific sequence of characters - for example to find all files that contain credit card numbers or passport numbers; and
*Subject Search:* which allows users to search for and locate specific information about a person or data subject (data from the uploaded contact lists).

***Network, Server and ECM Searching***

FileFacets uses custom connectors to access the unstructured data in Windows Shared Drives and various Enterprise Content Management systems. The Open Database Connectivity connector (ODBC) allows FileFacets to access structured systems built on SQL databases.

***Email Searching***

FileFacets scans and searches Microsoft Exchange servers and emails. It scans .eml files searching both the message text and any attachments. Attachments are represented in their native format with original file extensions. Messages and attachments are searched and indexed together to maintain message context.

***Desktop Searching***

The FileFacets Software Agent installed on a user's desktop allows access to, and scans for, personal data resident on employee's desktops and local drives - including any web-based file sharing systems (Dropbox, Google Drive) that are synced to the desktop. Desktop users have the ability to partition personal information (photos, videos, personal emails) from corporate information and can flag to exclude the personal content from future scans. The System Admin or Data Protection Officer (DPO) has the authority to override employee decision on the exclusion of personal data.

***Metadata Attribution***

When running a subject search of a contact list upload, FileFacets will search for and find all files that contain that individual's personal data and will flag it, or attribute metadata, to those files. When new files are created, FileFacets identifies which ones contains the personal data of each individual and automatically applies the corresponding metadata. The metadata stays with the file as it moves locations throughout the business, so no matter where it's moved to, you know where it is. This allows users to quickly find the data, regardless of its location, age or filetype, should an access request be made.

**Define Actions**

As businesses adopt privacy-centric processes and best practices as part of GDPR's Privacy by Design, FileFacets can implement those data handling decisions in an automated way. A user can define what rules or actions are to be taken for each file type (ex. contracts) or certain types of personal data (ex. passport numbers), and decide on how certain sensitive content is handled. For example, if there is an email containing a client's personal data on an employee's system: move it to a secure folder and delete it from source. Or, if an employee record is on a user's desktop: copy it to a secure HR folder and delete it from the desktop.

***Machine Learning***

FileFacets learns as it goes, dynamically clustering files or content into groups based on the content type or document type – allowing users to routinely action on that specific kind of data. When new content is added, FileFacets will find it, identify it, cluster it, and then action it, based on the defined business processes.

**Monitor**

FileFacets is used for ongoing compliance and monitoring of an enterprise's entire data stores. Admins and users can set up scheduled scans per file drive or repository at custom intervals: daily, weekly, monthly, quarterly, etc. Each time FileFacets performs a delta scan, any new or edited content is captured, and defined business rules and processes are applied to the new or edited content – ensuring all sensitive data within multiple sources are accounted for and flagged appropriately.

## FileFacets Solutions by Regulation Articles

The GDPR consists of 11 Chapter and 99 Articles:

Chapter 1: General Provisions

Chapter 2: Principles

Chapter 3: Rights of the Data Subject

Chapter 4: Controller and Processor

Chapter 5: Transfer of personal data to third countries of international organizations

Chapter 6: Independent Supervisory Authorities

Chapter 7: Co-operation and Consistency

Chapter 8: Remedies, Liability, and Sanctions

Chapter 9: Provisions relating to specific data processing situations

Chapter 10: Delegated Acts and Implementing Acts

Chapter 11: Final provisions

A Summary of associated Articles can be found on Page 16.

FileFacets can be used in a number of ways to solve for the data protection and information management requirements of a businesses' GDPR strategy: including Data Discovery & Data Protection, Risk Mitigation, Reporting, Data Subject Rights, and Information Governance.

FileFacets solves for the following Articles of the GDPR:

| Article | Title | Requirement | FileFacets will: |
|---|---|---|---|
| 12 | Transparent information, communication and modalities for the exercise of the rights of the data subject | A controller must, within one month of receiving a request made under data subject rights (Articles 15-22), provide any requested information in relation to any of the rights of data subjects. | ▪ Locate all files and records containing a subject's information across all systems<br>▪ QA results of search<br>▪ Copy files to 3rd party location for data export/secure data transfer to data subject |
| 15 | Right of access by the data subject | Data subjects have the right to obtain confirmation of where their personal data is being processed; the purposes of the processing, the categories of data being processed, whom the data may be shared, and the period for which the data will be stored. Additionally, data subjects may request a copy of the personal data being processed. | ▪ Locate all files and records containing a subject's information across all systems<br>▪ Identify the location of all documents that contain the subject's personal data<br>▪ View categories of personal data<br>▪ View rules-based actions for data (retention)<br>▪ QA results of search<br>▪ Copy files to 3rd party location for data export/secure data transfer to data subject |

| Article | Title | Requirement | FileFacets will: |
|---|---|---|---|
| 17 | Right to erasure ('right to be forgotten') | Data subjects have the right to erasure of personal data (the "right to be forgotten") if the data are no longer needed for their original purpose, the data subject withdraws that consent, or erasure is necessary for compliance with EU law or the national law of the relevant Member State. Excludes data that requires holding for legal, health or public interests. | ▪ Locate all files and records containing a subject's information across all data systems<br>▪ QA results of search<br>▪ Exclude documents required to be maintained for legal, health or public interest<br>▪ Delete files from source repository<br>▪ Provide audit reporting to confirm deletion |
| 18 | Right to restriction of processing | Data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes) | ▪ Locate all files and records containing a subject's information across all data systems<br>▪ Action documents or restrict permissions |
| 19 | Notification obligation regarding rectification or erasure of personal data or restriction of processing | The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, 17 and 18 to each recipient to whom the personal data have been disclosed. The controller shall inform the data subject about those recipients if the data subject requests it. | ▪ Locate all files and records containing a subject's information across all data systems<br>▪ Action documents or restrict permissions<br>▪ Copy files to 3rd party location for export to data subject<br>▪ Delete files from source repository<br>▪ Provide audit reporting to confirm deletion |
| 20 | Right to data portability | Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers. | ▪ Locate all files and records containing a subject's information across all data systems<br>▪ Copy files to 3rd party location for data export/secure data transfer |
| 24 | Responsibility of the controller | The controller is responsible for implementing appropriate technical and organizational measures to ensure and to demonstrate that its processing activities are compliant with the requirements of the GDPR. | ▪ FileFacets technology provides transparency and accountablility for data controllers and processors for GDPR. |

| Article | Title | Requirement | FileFacets will: |
|---|---|---|---|
| 25 | Data protection by design and by default | The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. | ▪ FileFacets as a tool in the protection and identification of data<br>▪ Locate all files and records containing a subject's information across all data systems<br>▪ Identify the location of all documents that contain the subject's personal data<br>▪ View categories of personal data<br>▪ View rules-based actions for data (retention) |
| 26 | Joint controllers | Joint controllers (where two or more controllers jointly determine the purposes and means of the processing of personal data) must, by means of an "arrangement" between them, apportion data protection compliance responsibilities between themselves (e.g., the responsibility for providing clear information to data subjects – see Chapter 9). | ▪ FileFacets allows for multiple admins or custodians over multiple jurisdicitons<br>▪ Reporting to track activity by each user to audit requests and search results |
| 27 | Representatives of controllers or processors not established in the Union | A controller established outside the EU must appoint a representative in one of the Member States in which the controller offers goods or services or monitors EU residents. | ▪ FileFacets allows for multiple admins and user access from multiple jurisdicitons<br>▪ Reporting to track activity by each user to audit requests and search results |
| 28 | Processor | A controller that wishes to appoint a processor must only use processors that guarantee compliance with the GDPR. | ▪ Allows data processor access to source repositories to ensure original data is not moved or altered |
| 29 | Processing under the authority of the controller or processor | The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller. | ▪ Reporting to track activity by each user to audit requests and search results |
| 30 | Records of processing activities | Each processor must keep records of its processing activities performed on behalf of the controller, including the categories of processing activities performed. | ▪ FileFacets allows for multiple admins and user access from multiple jurisdicitons<br>▪ Reporting to track activity by each user to audit requests and search results |

| Article | Title | Requirement | FileFacets will: |
|---|---|---|---|
| 33 | Notification of a personal data breach to the supervisory authority | In the event of a data breach, the controller must report the breach to the DPA within 72 hours of becoming aware of it. The notification must include at least a description of the data breach, including the numbers of data subjects affected and the categories of data affected. | ▪ Identify all documents that contain the subject's personal data in the system/area of the breach<br>▪ View number of data subjects and files affected by the breach<br>▪ View categories of personal data |
| 34 | Communication of a personal data breach to the data subject | In the event of a data breach causing high risk to data subjects, the controller must notify the affected data subjects without undue delay. The notification must include a decription of the data that was comprimised. | ▪ Identify all documents that contain the subject's personal data in the system/area of the breach<br>▪ Copy files to 3rd party location for data export/secure data transfer to data subject |
| 44-50 | Cross border data transfers | A transfer of personal data to a third country or international organization may take place where the third country or organization in question ensures an adequate level of protection. Cross-Border Data Transfers to a recipient in a third country may take place if there is consent given by the subject, or it is necessary for reasons of public interest or for the establishment, exercise or defence of legal claims. | ▪ FileFacets allows for multiple admins and user access from multiple jurisdicitons<br>▪ View and set rules-based actions for data actions and transfers<br>▪ Reporting to track activity by each user to audit requests and search results<br>▪ Copy files to 3rd party location for data export/secure data transfer to data subject between jurisdictions |
| 89 | Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes | Subject to appropriate safeguards, and provided that there is no risk of breaching the privacy of the data subject, Member States may restrict the data subject's rights to access, rectification, restriction of processing and to object when it comes to the processing of their personal data for scientific, historical or statistical purposes. | ▪ Locate all files and records containing a subject's information across all data systems<br>▪ QA results of search<br>▪ Exclude documents required to be maintained for other business purposes |

# Schedule A - GDPR: Summary of Articles

A full version of the GDPR Regulations can be found at: https://gdpr-info.eu/

**Chapter 1: General Provisions**
Article 1: Subject matter and objectives
Article 2: Material scope
Article 3: Territorial scope
Article 4: Definitions

**Chapter 2: Principles**
Article 5: Principles relating to personal data processing
Article 6: Lawfulness of processing
Article 7: Conditions for consent
Article 8: Conditions applicable to child's consent in relation to information society services
Article 9: Processing of special categories of personal data
Article 10: Processing of data relating to criminal convictions and offences
Article 11: Processing which does not require identification

**Chapter 3: Rights of the Data Subject**
*Section 1: Transparency and Modalities*
Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

*Section 2: Information and Access to Data*
Article 13: Information to be provided where personal data are collected from the data subject
Article 14: Information to be provided where personal data have not been obtained from the data subject
Article 15: Right of access by the data subject

*Section 3: Rectification and Erasure*
Article 16: Right to rectification
Article 17: Right to erasure ('right to be forgotten')
Article 18: Right to restriction of processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20: Right to data portability

*Section 4: Right to object and automated individual decision making*
Article 21: Right to object
Article 22: Automated individual decision-making, including profiling

*Section 5: Restrictions*
Article 23: Restrictions

**Chapter 4: Controller and Processor**
*Section 1: General Obligations*
Article 24: Responsibility of the controller
Article 25: Data protection by design and by default
Article 26: Joint controllers
Article 27: Representatives of controllers not established in the Union
Article 28: Processor
Article 29: Processing under the authority of the controller or processor
Article 30: Records of processing activities
Article 31: Cooperation with the supervisory authority

*Section 2: Security of personal data*
Article 32: Security of processing
Article 33: Notification of a personal data breach to the supervisory authority
Article 34: Communication of a personal data breach to the data subject

*Section 3: Data protection impact assessment and prior consultation*
Article 35: Data protection impact assessment
Article 36: Prior Consultation

*Section 4: Data protection officer*
Article 37: Designation of the data protection officer
Article 38: Position of the data protection officer
Article 39: Tasks of the data protection officer

*Section 5: Codes of conduct and certification*
Article 40: Codes of Conduct
Article 41: Monitoring of approved codes of conduct
Article 42: Certification
Article 43: Certification Bodies

**Chapter 5: Transfer of personal data to third countries of international organizations**
Article 44: General Principle for transfer
Article 45: Transfers of the basis of an adequacy decision
Article 46: Transfers subject to appropriate safeguards
Article 47: Binding corporate rules
Article 48: Transfers or disclosures not authorised by union law
Article 49: Derogations for specific situations
Article 50: International cooperation for the protection of personal data

**Chapter 6: Independent Supervisory Authorities**
*Section 1: Independent status*
Article 51: Supervisory Authority
Article 52: Independence
Article 53: General conditions for the members of the supervisory authority
Article 54: Rules on the establishment of the supervisory Authority

*Section 2: Competence, Tasks, and Powers*
Article 55: Competence
Article 56: Competence of the lead supervisory authority
Article 57: Tasks
Article 58: Powers
Article 59: Activity Reports

**Chapter 7: Co-operation and Consistency**
*Section 1: Co-operation*
Article 60: Cooperation between the lead supervisory authority and the other supervisory authorities concerned
Article 61: Mutual Assistance
Article 62: Joint operations of supervisory authorities

*Section 2: Consistency*
Article 63: Consistency mechanism
Article 64: Opinion of the Board
Article 65: Dispute resolution by the Board
Article 66: Urgency Procedure
Article 67: Exchange of information

*Section 3: European Data Protection Board*
Article 68: European Data Protection Board
Article 69: Independence
Article 70: Tasks of the Board
Article 71: Reports
Article 72: Procedure
Article 73: Chair
Article 74: Tasks of the Chair
Article 75: Secretariat
Article 76: Confidentiality

**Chapter 8: Remedies, Liability, and Sanctions**
Article 77: Right to lodge a complaint with a supervisory authority
Article 78: Right to an effective judicial remedy against a supervisory authority
Article 79: Right to an effective judicial remedy against a controller or processor
Article 80: Representation of data subjects
Article 81: Suspension of proceedings
Article 82: Right to compensation and liability
Article 83: General conditions for imposing administrative fines
Article 84: Penalties

**Chapter 9: Provisions relating to specific data processing situations**
Article 85: Processing and freedom of expression and information
Article 86: Processing and public access to official documents
Article 87: Processing of the national identification number
Article 88: Processing in the context of employment

Article 89: Safeguards and derogations relating to processing for archiving
purposes in the public interest, scientific or historical research purposes or statistical purposes
Article 90: Obligations of secrecy
Article 91: Existing data protection rules of churches and religious associations

**Chapter 10: Delegated Acts and Implementing Acts**
Article 92: Exercise of the delegation
Article 93: Committee procedure

**Chapter 11: Final provisions**
Article 94: Repeal of Directive 95/46/EC
Article 95: Relationship with Directive 2002/58/EC
Article 96: Relationship with previously concluded Agreements
Article 97: Commission Reports
Article 98: Review of other union legal acts on data protection
Article 99: Entry intro force and application