Ab Initio's Guide to Managing Personal Data for the GDPR

Ab Initio

Ab Initio’s Guide to Managing Personal Data for the GDPR

On May 25, 2018, when the EU’s General Data Protection Regulation (GDPR) becomes law, organisations could be fined up to 4% of their global annual turnover if they fail to comply. No matter where in the world you are, if you process, store, or transmit personal data on EU subjects — including customer and employee data — you must comply with the GDPR or risk fines and/or loss of business. The GDPR fundamentally broadens the definition of personal data and the protections accorded to data subjects; therefore, organisations will need to conduct comprehensive reviews of the personal data they have, where it is, how it is managed, and how it is governed.

The GDPR is still new, so organisations are still determining how they should interpret and implement GDPR’s requirements. Many, however, are behind and will need to catch up fast, as it appears regulators expect full compliance from day one. Some organisations have technologies in place that meet existing national data-protection laws, but in most cases, these will need to be enhanced to take into account the GDPR’s more stringent requirements.

The GDPR is a far-reaching regulation. There is no single technology or product that will solve all of GDPR’s challenges. Based on the breadth of the GDPR’s requirements, an individual organisation’s interpretations of them may differ according to their business models and/or environments. Most organisations will require individualised approaches to the GDPR that are supported not by “one-size-fits all” technology, but by flexible, yet comprehensive platforms that provide sophisticated personal data discovery, remediation, and control capabilities.

This paper outlines the GDPR’s requirements, explains the complex technological challenges organisations face when complying with the GDPR’s greatly enhanced personal-data protection expectations, and highlights some of the options available to address these challenges.

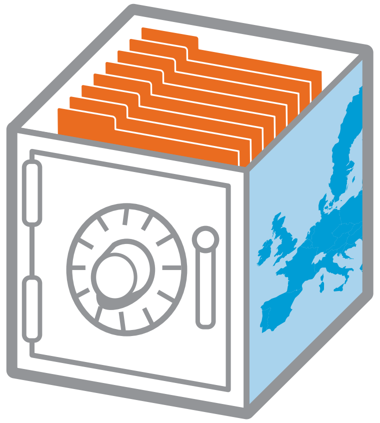
Ab Initio offers organisations a flexible platform for dealing with personal data that includes a comprehensive portfolio of data-governance, data-discovery, and data-protection capabilities that organisations worldwide already rely upon for their personal data management needs.

TABLE OF CONTENTS

Introduction to the General Data Protection Regulation (GDPR)

Universal respect for individual privacy is central to the EU's GDPR, which significantly extends the boundaries of personal data. Billed as a regulation to "arm the EU for the digital age,"[1] the GDPR centres on three key themes:

- Giving EU residents greater control over their personal data
- Protecting data subjects from corporate data breaches that result from weak security practices
- Facilitating commerce in the EU zone by enabling the smooth transfer of data — unimpeded by conflicting national laws — between organisations in member states or select countries outside the EU



There's no grace period when the GDPR goes into effect: any organisation that wants to operate within or trade with the EU must be fully compliant. Steve Wood of the UK Information Commissioner's Office made this point clear in his keynote at the IAPP's 2017 Data Protection Intensive.[2]

When the GDPR goes into effect, it will replace the national legislation of EU member states, including the UK's Data Protection Act 1998, France's Loi Informatique et Libertés (LIL), Germany's Bundesdatenschutzgesetz (BDSG), and similar privacy regulations in all other EU member states. Aiming to harmonise differences between national laws, the GDPR also introduces some key changes, including:

- **A broader definition** of personal data that includes "any information relating to an identified or identifiable natural person ('data subject')"[3] as well as any data that could be leveraged or combined to identify an individual.
- **Proof of affirmative consent** for every usage (processing purpose) of personal data. If a company wants to carry out six different actions with the subject's data, it needs to ensure that the data subject has consented to each of them.
- **Thirty days to fulfil Subject Access Requests (SARs)**, which means that entities in some jurisdictions will have less time to fulfil SARs. All organisations must meet additional disclosure requirements — including the disclosure of all processing objectives and any third parties that received a subject's data — and do so in clear language that the subject can understand, even if he is a child. [4]
- **The Right to be Forgotten,** which means that data subjects can request that their data be erased or rendered un-processable.
- **Data Portability,** which means that data subjects can take their data to new providers. Conversely, your new customers will be able to bring you data from their previous data providers.
- **Seventy-two-hour breach notification,** required in the event of personal-data breaches.
- **Data Protection Officer (DPO),** a position required in entities whose core activities include regular and systematic monitoring of data subjects on a large scale or in organisations that process special data categories.
- **Privacy by design and data minimisation.** A subject's privacy must be the starting point for all system design. Companies must build privacy rules and processes into systems. Companies must not store more data than that required for the consented processing purpose.

Because the GDPR scope encompasses organisations monitoring the behaviour of individuals, it applies to numerous companies. Almost every website and app captures the activities of users in one way or another.

Does the GDPR Apply to Companies Based Outside the EU?

The GDPR is far-reaching. It applies to the personal data of all EU residents, regardless of where their data resides. This means the impact on organisations is global. Many non-European organisations assume that the GDPR does not apply to them. No matter where in the world your organisation is based, if you process, transmit, or store data for — or about — EU residents, you are expected to comply with the GDPR. Thus, even a B2B transaction between two non-EU entities could be deemed subject to the GDPR if the transaction involves use or transmission of personal data of an EU data subject. Moreover, the European Commission has empowered its authorities to pursue GDPR violators worldwide, regardless of their country of origin.

Even if you are not operating in the EU, European authorities will consider the GDPR to be applicable if you process (which includes receiving and, if applicable, storing) the personal data of European residents so as to offer goods or services, or monitor the behaviour of EU residents.

Summary of Key GDPR Principles

KEY GDPR PRINCIPLES	IMPLICATIONS
Personal data must be collected for specified, explicit, and legitimate purposes	• Personal data collection, storage, and processing must comply with, and be limited to, the exact purpose for which consent was provided. • The GDPR's data retention rules for deleting unused personal data must be balanced against tax and other regulations that may require its retention.
Personal data may only be collected and processed for: • Performance of legal obligations • Execution of a contract with the data subject • A purpose for which the data subject has given specific consent	• A company must do the following: • Inventory its personal data holdings and usage. • Stipulate policies to govern the specific usages of personal data, according to consent collected from the data subject. • Implement data control and protection measures to implement/ enforce those consents and prevent the misuse of personal data.
Personal data must be adequate, relevant, and not excessive	• Personal data should only be stored and processed to the extent, and where, it is needed. • Companies must eliminate — and not collect — excess personal data that is not strictly necessary according to the processing purpose.
Personal data must be accurate and, where necessary, kept up to date	• Personal data quality must be assessable and monitored, and data quality issues identified and remediated.
Identifiable personal data must not be kept for longer than required, and data subjects have the right to be forgotten	• Data subjects can request that companies erase their personal data. • Consent agreements should state how long personal data is retained. • Where consent is withdrawn, or the retention period elapses, personal data should be rendered "un-processable," unless legal requirements dictate otherwise. • Periodic or continuous audits are required to ensure that personal data is not kept longer than required.
Data subjects have the right to: • Request information about their own personal data and its usage • Take their data to another firm	• The Chief Data Officer should be able to produce a list of usages — in an intelligible format — to the data subject upon request, without undue delay. • Data subjects may request that their data be provided in a portable data format.
The data controller is accountable for third-party storage and processing of personal data	• Governance and traceability requirements extend to any third-party data processors to which the firm (data controller) has delegated data processing. • When a data subject requests information about her data, the data controller must provide information about any third-party contractors with access to the data.

*These principles are based on Article 5 of the General Data Protection Regulation of April 27, 2016.

Discover, Remediate, Control

Given the breadth of GDPR requirements, organisations are facing monumental challenges. Ab Initio can help.

GDPR compliance can be approached in three phases:

DISCOVER
Find personal data and the basis for processing

REMEDIATE
Minimize and protect data, Update systems

CONTROL
Monitor and analyse data requests and usage

- **Discover** — Before organisations can design a data-governance infrastructure that complies with GDPR, they need to identify and catalogue the personal data they possess and the basis of consent for processing. This means:
  - Define personal data. Identify sensitivity categories, create business dictionaries, and formulate policies and controls.
  - Take inventory. Scan and construct an inventory of business systems. Construct and map business and technical data lineages.
  - Perform personal data discovery. Identify where sensitive data is held within those systems.
- **Remediate** — Once personal data is discovered and catalogued, organisations can begin to implement remediation processes to ensure compliance. This means:
  - Minimise data. Eliminate redundancy. Employ deduplication. Delete data not covered by, or surplus to, consents.
  - Protect data. Apply security policies. Mask, encrypt, and tokenise data.
  - Implement control checks. Enforce application of consent, data quality, and security policy checks, as well as data retention policies for key systems.
- **Control** — Organisations will need to:
  - Analyse new systems.
  - Periodically re-run personal data cataloguing and discovery.
  - Fulfil SARs.
  - Manage processes concerning the right to be forgotten, breach identification and reporting, and consent management.

Ab Initio provides a wide range of technologies for data governance, personal data discovery, data protection, and data quality that can be combined to help organisations address the GDPR's requirements.

DISCOVER

As the regulation itself states, organisations must appoint a Data Protection Officer and establish a Data Protection Office. The Data Protection Officer will need to define and formalise roles and responsibilities, define the organisation's governance structure and processes, and establish GDPR programme goals and success criteria, as well as funding and resources.

Most compliance teams begin their GDPR programmes by documenting the organisation's personal data usage and the basis for processing it. During the discovery phase, organisations need to:

- **Define** the organisation's programmes, accountabilities, and governance framework required to support personal data discovery and GDPR remediation activities.
- **Discover** the extent and locations of personal data the organisation holds and the paths through which it receives new personal data.
- **Inventory** or catalogue the systems that contain personal data and their basis for processing.

Define

Organisations should prepare themselves before discovering personal data by completing the following activities, which will maximise their discovery efforts and save time and resources later:

Under the GDPR, organisations whose core activities require "regular and systematic monitoring of data subjects on a large scale" or that process special categories of data on a large scale require an executive — the Data Protection Officer — who functions as a "mini-regulator."

That individual's duties are similar to those of a compliance officer, but he or she also needs skill in managing cybersecurity, data breaches, IT processes, and business continuity issues.

- Define the principles, goals, policies, and practices that constitute the organisation's GDPR programme
- Define what the organisation deems to be personal data, and create a business glossary
- Assign data stewards in order to allocate tasks to them
- Create sensitivity categories for personal data

Defining Your GDPR Programme: Principles, Policies, Plans, and Practices

As organisations begin their GDPR compliance initiatives, they will want to define and document (and later, manage) the principles, policies, plans, accountabilities, and practices for GDPR governance. While this may seem a daunting task, an effective approach is to begin with the GDPR principles themselves.

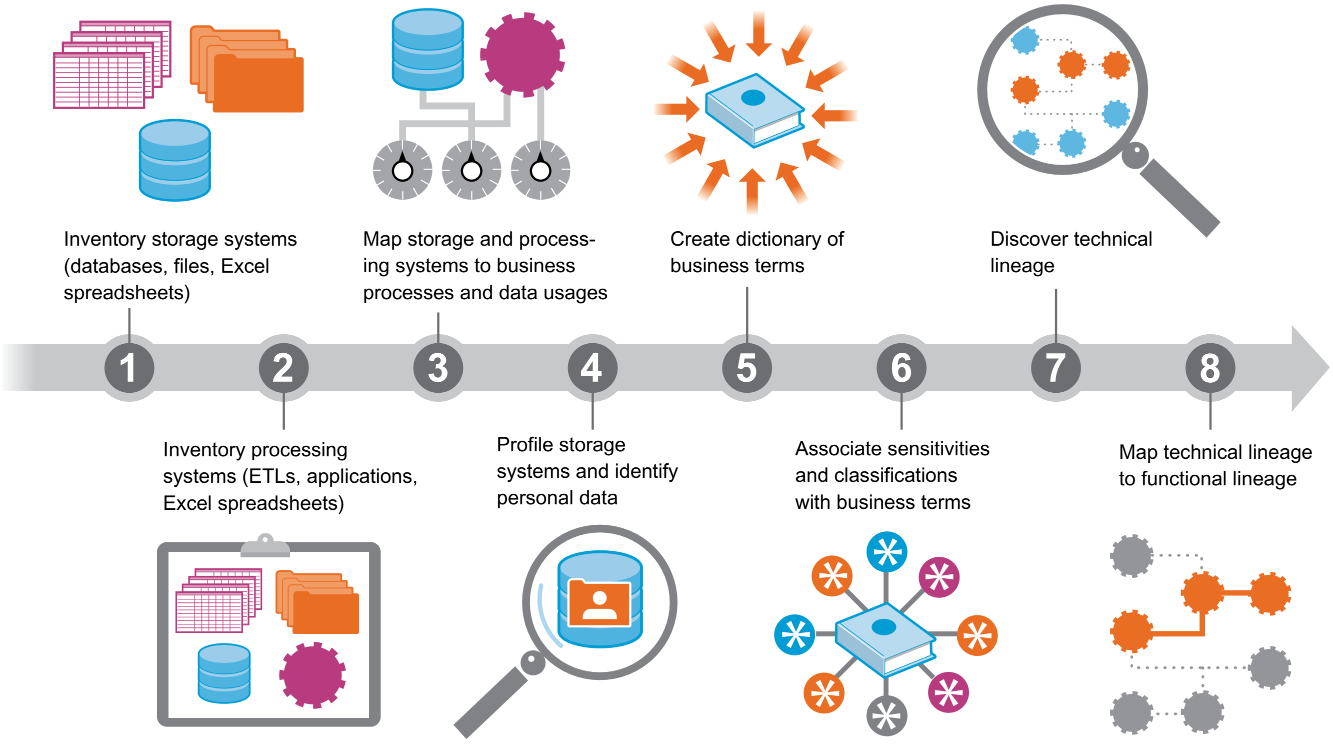
Article 5 of the GDPR — "Principles relating to processing of personal data"[5] — summarises many of the key themes of the regulation. The principles include:

- Lawfulness, Fairness, and Transparency of Processing (processing basis)
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation (limited retention period)
- Integrity and Confidentiality (data protection for data subjects)

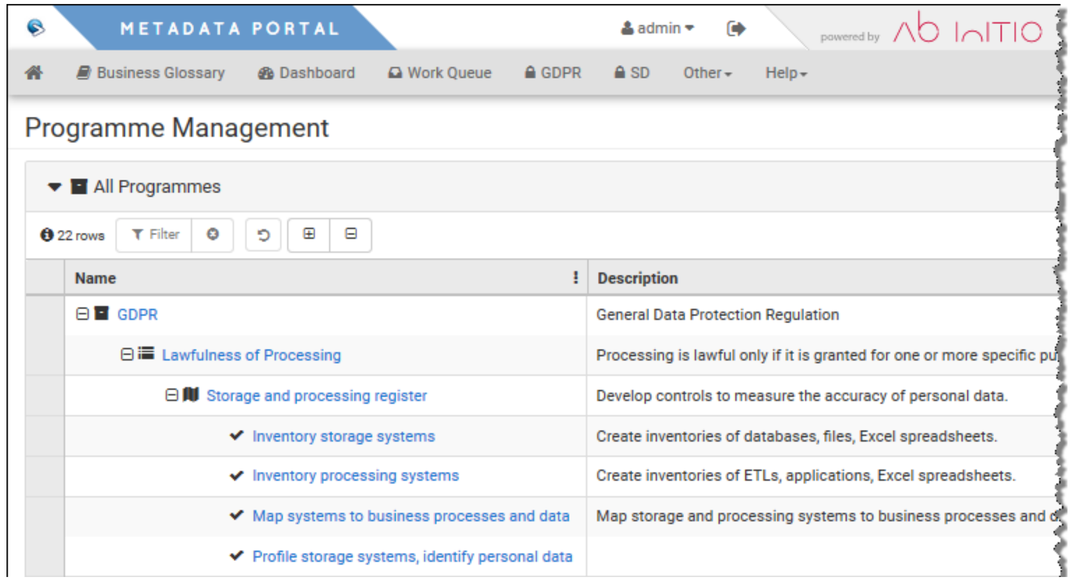
These principles can be treated as a high-level starting point that enables you to define plans for measurement, monitoring, issue remediation, and ongoing compliance. Organisations can accomplish this by implementing:

- **Policies** — Documenting organisational policies based on the principles
- **Plans** — Breaking down the policies/principles into plans that state courses of action
- **Steps** — Documenting the tasks people need to perform to complete the plan (or continuously achieve it) and assigning ownership to those tasks

For example, to meet the "Lawfulness of Processing" principle, organisations could define a plan to create a "Storage and processing register." The steps required might include, for example:


1
Inventory storage systems (databases, files, Excel spreadsheets)
2
Inventory processing systems (ETLs, applications, Excel spreadsheets)
3
Map storage and processing systems to business processes and data usages
4
Profile storage systems and identify personal data
5
Create dictionary of business terms
6
Associate sensitivities and classifications with business terms
7
Discover technical lineage
8
Map technical lineage to functional lineage

The following screen capture provides an example of how an organisation might instantiate this process by using Ab Initio software:



Programme Management

All Programmes

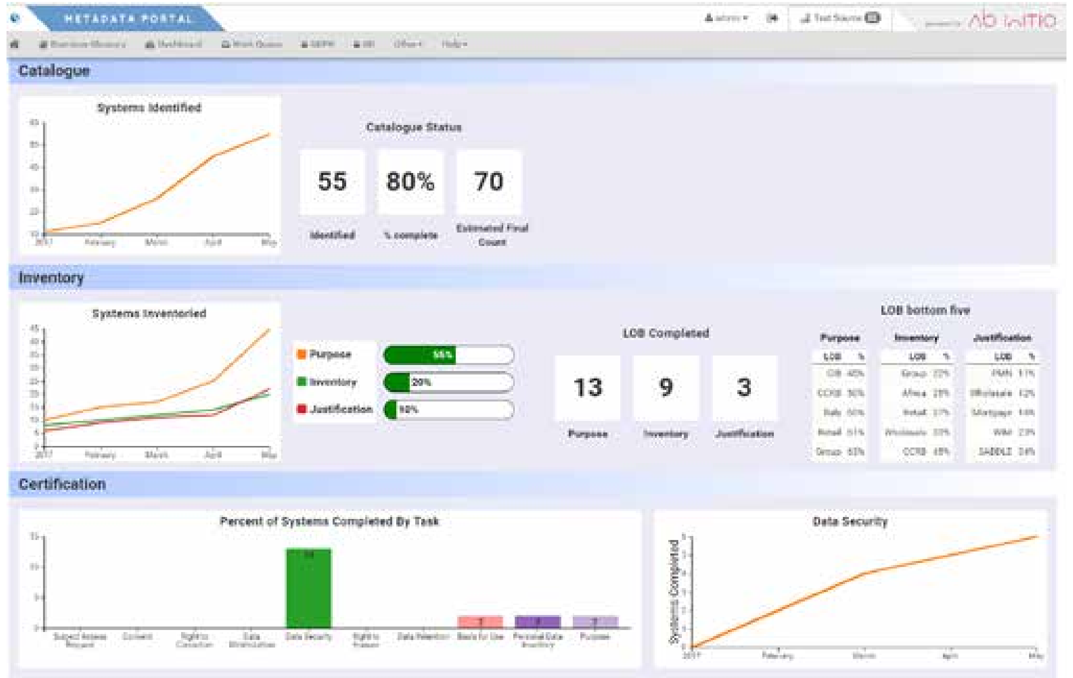
22 rows

Name	Description
GDPR	General Data Protection Regulation
Lawfulness of Processing	Processing is lawful only if it is granted for one or more specific pu
Storage and processing register	Develop controls to measure the accuracy of personal data.
✓ Inventory storage systems	Create inventories of databases, files, Excel spreadsheets.
✓ Inventory processing systems	Create inventories of ETLs, applications, Excel spreadsheets.
✓ Map systems to business processes and data	Map storage and processing systems to business processes and d
✓ Profile storage systems, identify personal data	

Steps can represent recurring processes. For example, you could have steps for designing data quality tests and determining whether they are fit-for-purpose, as well as a process for handing an application over to quality assurance for testing.

Defining and documenting your GDPR programme in this way not only provides effective management for your organisation's people, but also creates documentation that can be shown to regulators, demonstrating that you have formal, repeatable processes in place to ensure compliance. (In some situations, regulators may be as interested in auditing an organisation's processes as in investigating the data related to a breach or a data subject's complaint.)

Ab Initio provides an effective method of managing this process, integrating policies, plans, and steps with data stewards, as well as providing dashboards and insight into the actual data itself.



Defining Personal Data and Creating a Business Glossary

During the 2014 Yahoo breach, hackers stole users' names, email addresses, phone numbers, dates of birth, and encrypted passwords. The hackers did not, however, abscond with credit card numbers or other financial information — a traditional focus for cybersecurity. Instead, they took personal data, possibly so they could leverage it to manufacture credentials and log in to other non-Yahoo accounts of those users.[6]

In the last three years, it's become clear that malefactors can exploit personal data that was previously seen as unimportant to secure. Consequently, it's not surprising the GDPR extends the definition of personal data to any information related to the identification of a data subject. Examples include personal data collected when registering for a library card, signing up for a gym membership, opening a bank account, etc.

The GDPR deems personal data to be any data that could be leveraged or combined to identify an individual. ("Just knowing a birthdate, gender and ZIP code is enough information to identify as many as 87 percent of people in the United States," according to data-privacy professor Latanya Sweeney of Harvard University.[7])

Note that names are not necessary for data to be designated as personal. The GDPR considers location data, identification numbers, radio-frequency identification (RFID) tags, or online identifiers such as IP addresses or cookies to be personally identifiable information.

Defining Personal Data in Your Organization

Although the GDPR provides examples of what it considers personal data, it does not provide an exhaustive list. Therefore, each organisation must decide and define what constitutes personal data in its own business.

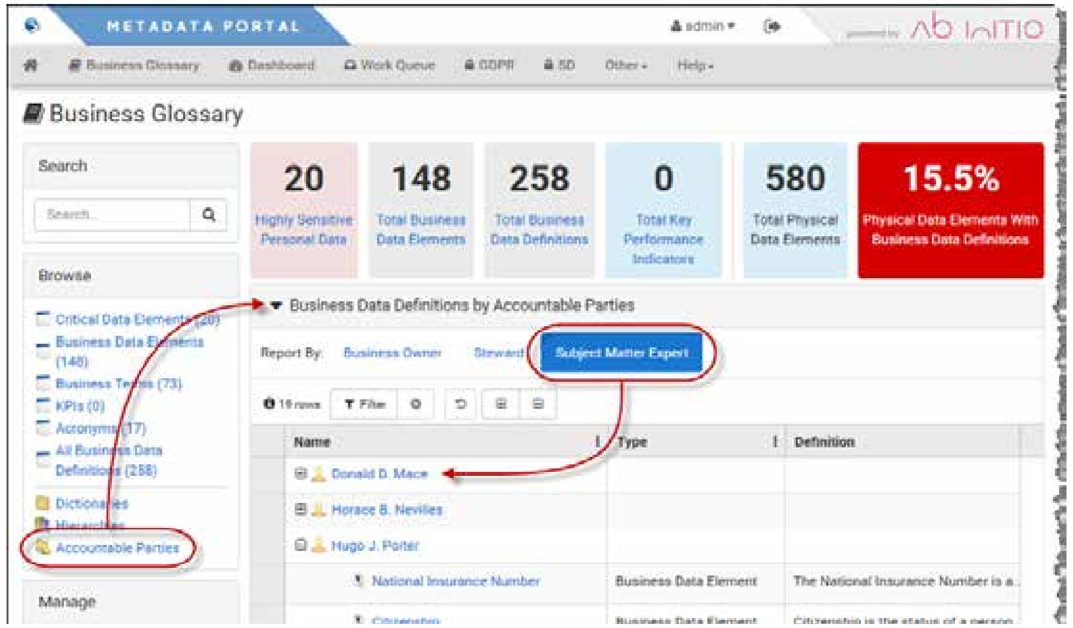
You will probably begin this process by defining a generic list of business terms for inclusion in your compendium of personal data, such as:

Credit Card Number/Account Number
Full Name/First Name/Last Name
Home Address/Email Address
National Identification Number
Vehicle Registration Plate Number
Passwords
Passport Number
IP Address

Date of Birth
Birthplace
Driver's License Number
Telephone Number
Race
Religion
Name of School/Workplace

Ab Initio's data-governance system includes rich business-glossary capabilities and supports the linking of business terms to physical data elements.

Ab Initio's business glossary supports complex, flexible hierarchies that enable you to categorise any business terms your Subject Matter Experts define according to the expert's area — for example, you can organise business terms by department (Marketing, Transactions, or Procurement) or application area.



Business Glossary

20	148	258	0	580	15.5%
Highly Sensitive Personal Data	Total Business Data Elements	Total Business Data Definitions	Total Key Performance Indicators	Total Physical Data Elements	Physical Data Elements With Business Data Definitions

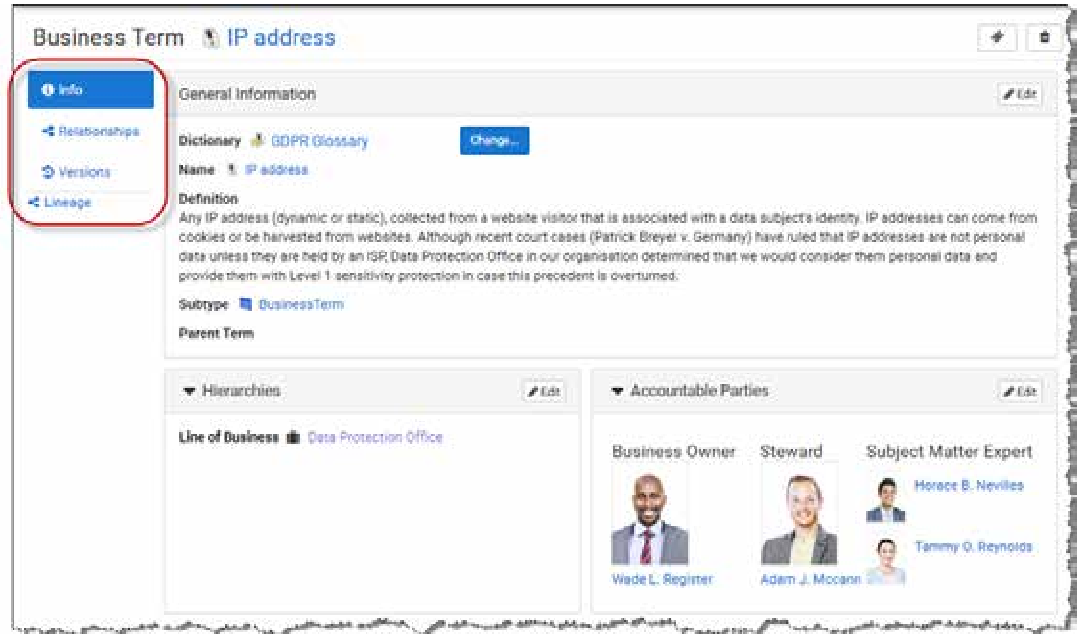
Business Data Definitions by Accountable Parties

Name	Type	Definition
Donald D. Mace		
Horace B. Nevilles		
Hugo J. Porter		
National Insurance Number	Business Data Element	The National Insurance Number is a...
Citizenship	Business Data Element	Citizenship is the status of a person...

Assigning Data Stewards and Other Accountable Parties

The GDPR differs from other data-governance regulations in that it requires a significant amount of matrix management and cross-team collaboration. Unlike regulations for banking risk, for example, the GDPR potentially encompasses a far broader set of departments, including Human Resources, Legal, Procurement, Marketing, Engineering, Product Management, Information Security, Website Development, and others. Any department that deals with any type of personal data — including vendor, consumer, customer, employee, or contractor — is likely one whose activities will be subject to the GDPR.

Working with data owners and other stakeholders across internal organisational boundaries makes it difficult to manage responsibilities cross-functionally. Organisations require strong supporting technology to manage the various accountable parties and the tasks and responsibilities assigned to them.



Business Term IP address

General Information

Dictionary GDPR Glossary

Name IP address

Definition
Any IP address (dynamic or static), collected from a website visitor that is associated with a data subject's identity. IP addresses can come from cookies or be harvested from websites. Although recent court cases (Patrick Breyer v. Germany) have ruled that IP addresses are not personal data unless they are held by an ISP, Data Protection Office in our organisation determined that we would consider them personal data and provide them with Level 1 sensitivity protection in case this precedent is overturned.

Subtype BusinessTerm

Parent Term

Line of Business Data Protection Office

Business Owner	Steward	Subject Matter Expert
Wade L. Register	Adam J. Mccann	Horace B. Nevilles Tammy O. Reynolds

Creating Sensitivity Categories for Personal Data

The GDPR designates special (or "sensitive") categories of personal data as meriting higher protection and a more stringent processing basis (or justification) than others.

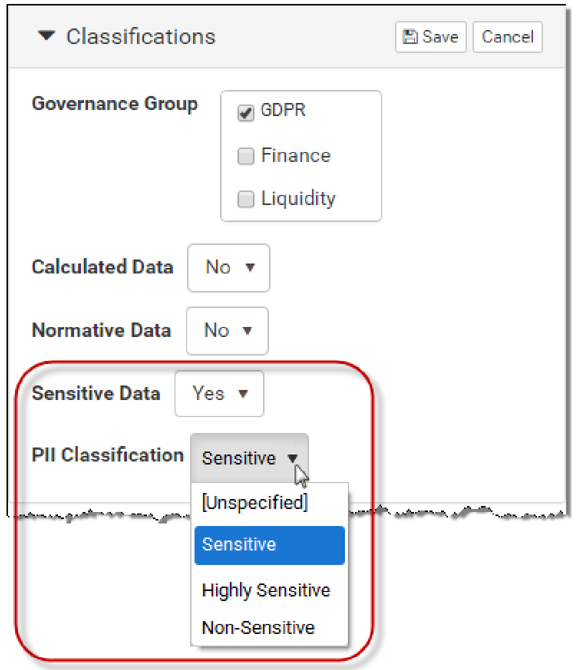
Examples of such information include data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual orientation, health information, and genetic or biometric information. Furthermore, certain types of sensitive data, including that containing health, biometric, or genetic data, can be processed only for limited purposes that benefit the data subject or public health.

Organisations need to establish sensitivity categories for personal data, such as:

- **Highly Sensitive Data** — Information that is restricted from automated decision making or that is particularly vulnerable to breaches, such as biometric, genetic, or health information; children's personal information; and financial or payment information.
- **Sensitive PII** — Any data used in high-risk processing — that is, data that, were it revealed, could lead to discrimination — such as religion, racial, or ethnic information; trade-union membership; information about sexual orientation; or political opinions.
- **Non-Sensitive PII** — Publicly available personal information, such as phone numbers and addresses.

Organisations need to track personal data in a way that not only supports the display of its sensitivity classification, but also facilitates prioritisation by enabling the grouping of issues according to the data's sensitivity.

Existing industry regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), require their own sensitivity categories and/or variations to the above, adding further complexity. Ab Initio software readily supports fine-grained sensitivity classifications, ensuring effective management of personal data.



▼ Classifications

Save | Cancel

Governance Group: ☑ GDPR ☐ Finance ☐ Liquidity

Calculated Data: No ▾

Normative Data: No ▾

Sensitive Data: Yes ▾

PII Classification: Sensitive ▾

[Unspecified]
Sensitive
Highly Sensitive
Non-Sensitive

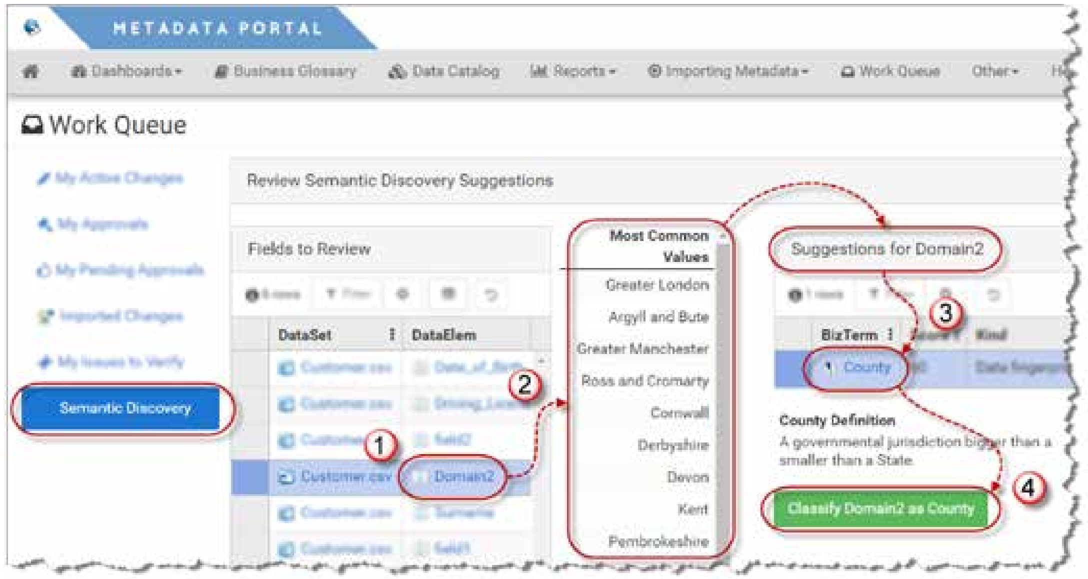
Organisations can configure whatever sensitivity classifications for data they want, including the ones shown.

Discover

During discovery, you may find that you are processing more personal data than you previously realized. Under the GDPR's broad definition of personal data, IP addresses, mobile device IDs, location data, and other unique identifiers may be considered personal data in some contexts. Furthermore, the extent of your personal data holdings may surprise you; personal data may have been replicated to numerous locations, including backup databases, document servers, and local computers.

To discover the nature and extent of their personal data holdings, organisations require sophisticated data discovery capabilities, such as those provided by Ab Initio software, that identify:

- **Personal data** in structured, semi-structured, and in some cases unstructured sources, including files, databases, SAS and other code libraries, Hadoop and big data files, plus datasets in other formats
- **Patterns in data** that indicate that personal data is probably present
- **Disparate data** that, when linked together, could constitute personal data (often referred to as "linkable" data)



Work Queue

Review Semantic Discovery Suggestions

Fields to Review

DataSet	DataElem
Customer.csv	Date_of_Birth
Customer.csv	Driving_Lic...
Customer...	field2
Customer.csv	Domain2
Customer.csv	Surname
Customer.csv	field1

Most Common Values
Greater London
Argyll and Bute
Greater Manchester
Ross and Cromarty
Cornwall
Derbyshire
Devon
Kent
Pembrokeshire

Suggestions for Domain2

BizTerm	Score	Kind
County	80	Data fingerpr...

County Definition

A governmental jurisdiction bigger than a smaller than a State.

Classify Domain2 as County

Ab Initio enables data stewards to understand the contents of (1) vaguely named fields (or data elements) by (2) showing them a preview of the field's most common values, (3) suggesting a business term that corresponds with the field, and (4) letting data stewards confirm the link between the business term/data element at the click of a button.

By using a combination of different techniques, the most capable data discovery technologies will be able to intelligently detect where a field contains personal data. These techniques include:

- **Metadata pattern analysis** — Analysing dataset descriptions to intelligently search field, column, file, and table names and descriptions for text that implies an association with personal data. For example, this technology may be used to search for "customer name" fields. When it detects potential matches — regardless of whether they are named CUST_NAME, CNAME, CSTNM, or another variant — it scores those fields to indicate the strength of the potential match.

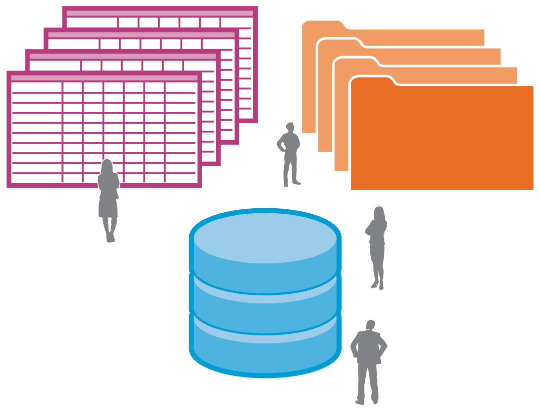
- **Data pattern scanning** — Scanning the contents of fields and columns for patterns, a methodology augmented by sophisticated, patented statistical and algorithmic techniques. Analysing these patterns suggests the nature of the data — for example, by identifying when a field contains address data. Although discovery contains specific patterns for many different types of personal data — such as national identification numbers, credit card numbers, phone numbers, and first names — matching should not be limited to such patterns. Rather, discovery should "learn" your data's specific data classifications, and search for them.
- **Rule-based analysis** — Running rules against the data's contents to determine whether predefined patterns and structures, which may indicate the presence of personal data, exist. For instance, a rule representing the patterns and structures of a credit card number might be tested against the data.

When used in unison, these approaches — which Ab Initio employs — ensure the best possible success in identifying personal data.

For many organisations, Ab Initio's discovery technology is a game changer. It makes it possible to automate the process of identifying where personal data is held across the enterprise — a task that might otherwise take years or simply not be possible.

Ab Initio can improve the way in which organisations approach GDPR compliance by offering a flexible and sustainable solution that maximises efficiency, reduces the need for manual data investigation, and identifies the personal data the organisation processes.

Inventory



The GDPR dictates that data subjects must actively consent to having their personal data processed, unless there is a (legal) basis for the use of the data without consent. Furthermore, the nature of data processing activities must not violate the GDPR.

Consequently, the GDPR implies that organisations will need to review their personal data processing activities in order to:

- **Document the basis for processing** each category of personal data, across all systems.

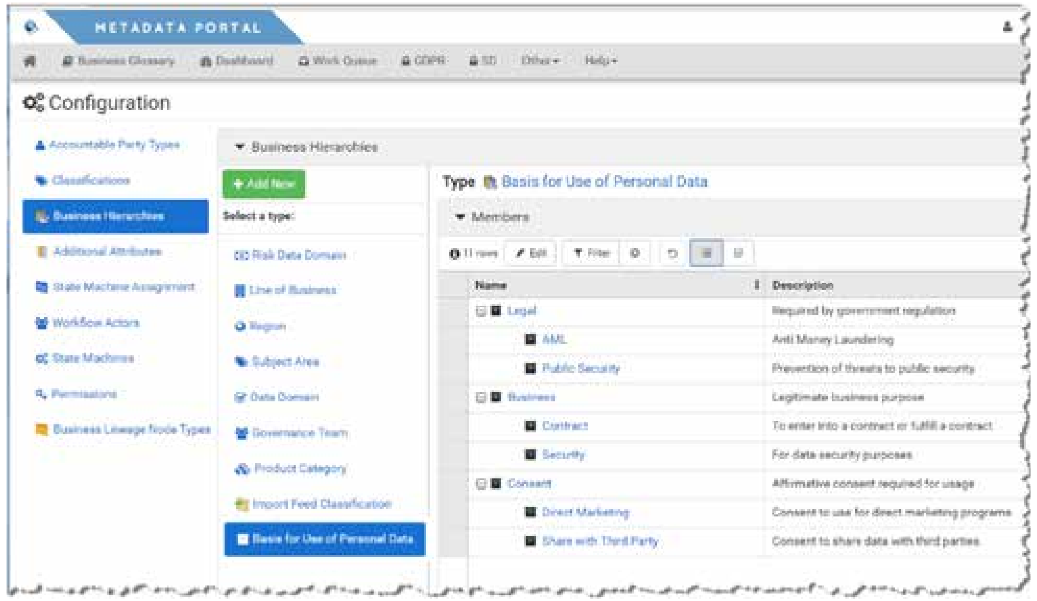
  Not all processing requires consent. Consent is required only when data subjects have a genuine choice over the processing, such as when it is for marketing purposes. Consent is not required when personal data is used in business transactions inherent to the business, such as a customer address used for shipping or billing purposes.

  It is important to encapsulate the types of usage that your enterprise has for personal data — for instance, "Marketing" or "Insurance Risk Calculation" — and to map this against the systems that implement these usage types.

- **Catalogue the purpose of each data processing system** (create a "process registry").
- **Determine whether unnecessary personal data is held** in databases and systems beyond what is necessary for the system's purpose:
  - If consent does not cover a system's usage of personal data (or its actual purpose in practice), you may need to re-obtain consent.
  - If a system contains excessive personal data or data that is not relevant, that data will probably need to be removed.
- **Evaluate whether any existing data processing violates the GDPR**. For instance, automated decisions cannot be based on special classes of data such as race or sexual orientation.
- **Verify that the existing mechanisms for obtaining consent meet GDPR requirements**. For example, under the GDPR, data subjects must actively provide consent. Agreement checkboxes cannot be preselected. People must opt in, not out. And website disclaimers that cookies store IP addresses may no longer constitute a valid form of consent. Existing mechanisms for obtaining consent created under the 1995 European Data Protection Directive may still be valid, but given the increased scope of the GDPR, organisations should review these mechanisms and agreements.

Ab Initio software enables organisations to inventory and track personal data processing by:

- **Using data lineage** to create a process inventory, identifying how personal data flows through your systems.
- **Identifying which applications** create and process personal data and which applications consume it.
- **Creating and managing the taxonomy** of basis for use (consented use types) — that is, those usage types for which a data subject's permission is sought. Ab Initio's graphical business and technical data lineages enable organisations to easily identify which systems require each consented usage type.



Configuration

Business Hierarchies

Select a type:

Type Basis for Use of Personal Data

Members

Name	Description
Legal	Required by government regulation
AML	Anti Money Laundering
Public Security	Prevention of threats to public security
Business	Legitimate business purpose
Contract	To enter into a contract or fulfill a contract
Security	For data security purposes
Consent	Affirmative consent required for usage
Direct Marketing	Consent to use for direct marketing programs
Share with Third Party	Consent to share data with third parties

Ab Initio software enables organisations to create various classifications for consent, which are applied to systems.

Some examples include:

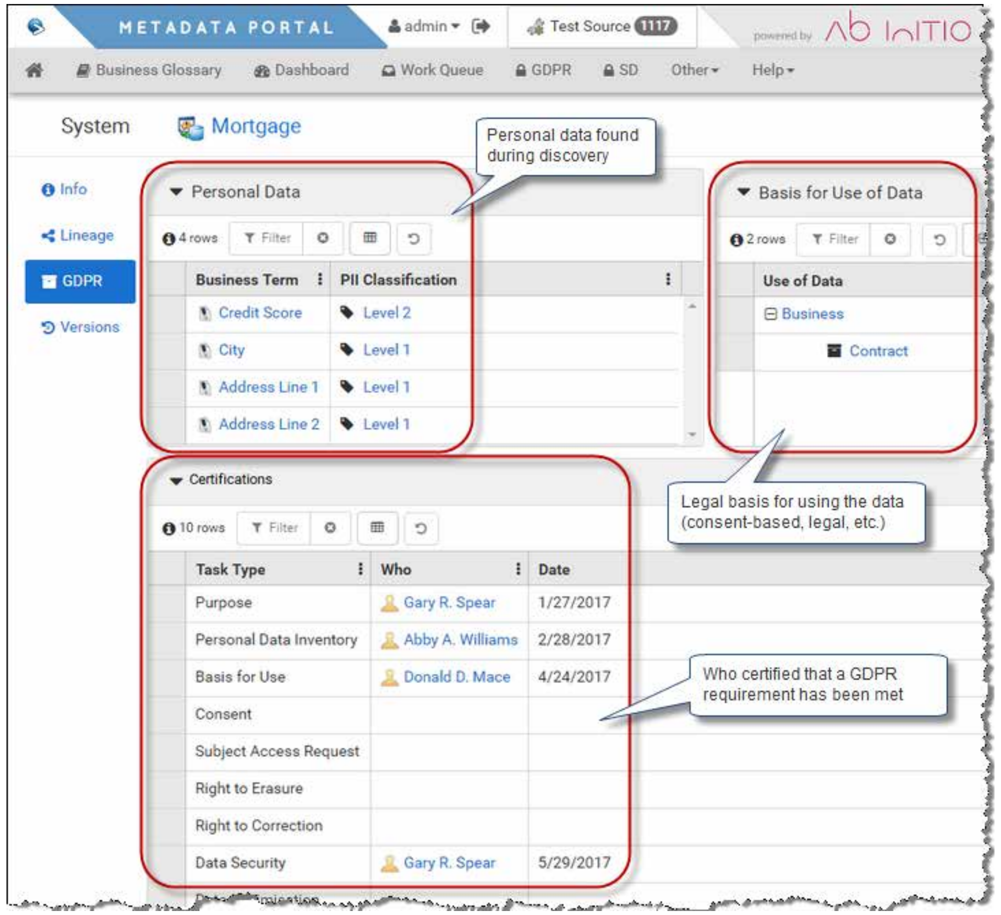
- Does Not Require Consent (Lawful Basis)
- Requires Affirmative Consent
- Requires Explicit Consent to Process (Highly Sensitive Data)
- Requires Explicit Parental Consent to Process (Children's Data)

- **Managing the association** between consented use types and the system implementations of those uses. For any given system, Ab Initio software can be configured to display the basis for use of the data and who certified that the system complies with that basis for use.
- **Capturing the processing purpose,** per system and per consented use type. This includes descriptions of the nature of the data processing being performed, together with the legal justification for processing.

Should an organisation identify instances of personal data processing for which active consent is required but has not been obtained, Ab Initio includes full issue management and remediation workflow capabilities to address problems through to resolution.

As the organisation analyses its personal data and creates inventories, it should note areas in which validation processes (manual or automated controls) need to be created — ensuring that the organisation is meeting its GDPR requirements. Such controls can be set up in Ab Initio.

At the end of the data discovery and inventory process, Ab Initio software will be able to display the results of your discovery efforts in one consolidated screen for each system. For example, the GDPR page for the Mortgage System shows the Personal Data found during data discovery, the system's basis for use of that data, and a summary of completed remediation steps.



System Mortgage

Personal data found during discovery

Personal Data

4 rows

Business Term	PII Classification
Credit Score	Level 2
City	Level 1
Address Line 1	Level 1
Address Line 2	Level 1

Basis for Use of Data

2 rows

Use of Data
⊟ Business
Contract

Legal basis for using the data (consent-based, legal, etc.)

Certifications

10 rows

Task Type	Who	Date
Purpose	Gary R. Spear	1/27/2017
Personal Data Inventory	Abby A. Williams	2/28/2017
Basis for Use	Donald D. Mace	4/24/2017
Consent		
Subject Access Request		
Right to Erasure		
Right to Correction		
Data Security	Gary R. Spear	5/29/2017

Who certified that a GDPR requirement has been met

After data stewards complete tasks captured in the Programme page and the stewards certify that the requirement is met, the completed items appear as Certifications on the system's GDPR page.

REMEDIATE

Once organisations understand their personal data holdings, they will probably need to engage in remediation activities, modifying some of their systems to make them compliant with the GDPR. The GDPR discovery may have revealed that:

- One or more systems hold too much or unnecessary personal data.
- Applications may be passing personal data to systems that are not permitted to use that data.
- Systems may duplicate existing functions and, consequently, serve as repositories of unnecessary personal data.

Likewise, you may determine that you want to redesign systems and implement new processes to ensure that you proactively meet the GDPR's requirements in future.

Some GDPR requirements, such as data minimisation, will result in a significant amount of work as you bring your environment into compliance. To sustain that compliance, however, will require ongoing maintenance processes to ensure problems don't recur.

Other remediation tasks, such as evaluating the risks associated with specific personal data and the need to secure that data, are not strictly required by the GDPR but rather are strongly encouraged.

In some cases, organisations will want to create new applications and processes to help them ensure compliance going forward, during operations. Examples include consent-based processing or data quality processes to ensure that data is accurate.

Ultimately, remediation is more than just modifying systems — it's about proactively creating ways to reduce issues and associated correction tasks in the future.

Minimising Unnecessary Personal Data

The GDPR requires that the processing of personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which [the data is] processed ('data minimisation')."[8]

Minimising the storage of data and minimising personal data can be a complicated undertaking involving significant systems analysis and change.

Ab Initio software can help in two key ways:

- The platform enables rapid identification and analysis of where personal data is stored and how it is used. This assists in the process of impact assessment.
- Ab Initio's discovery and pattern-matching technologies enable the identification of duplicate or potentially duplicate data.

If analysts determine that excessive personal data results from too much data being collected from your customers (the data subjects), Ab Initio's platform can trigger a remediation process that prompts other teams to update web forms.

Evaluating the Risk of Personal Data and Securing It

Many companies are reluctant to encrypt or otherwise obscure their data. Under the GDPR, however, encryption and obfuscation become a form of insurance against reputational damage from data breaches.

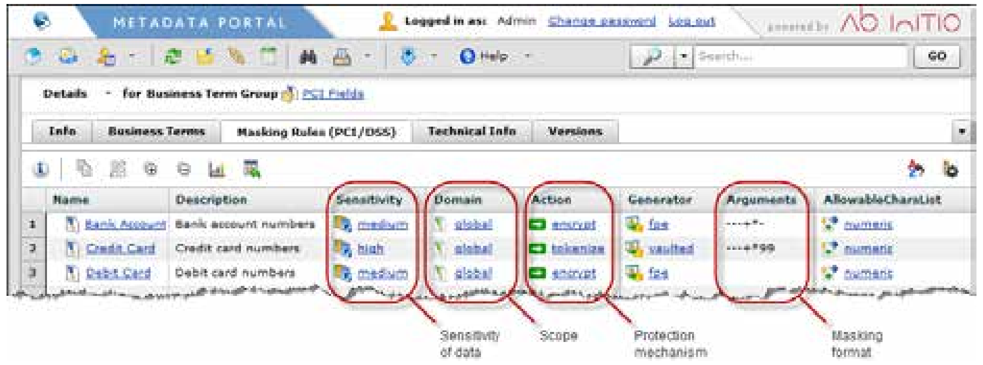
Although the GDPR doesn't dictate that organisations must encrypt personal data, the regulation encourages them to do so in its provisions for data breaches. If companies don't take appropriate technical and organisational measures to protect personal data, they have just 72 hours to inform the regulator and affected data subjects of breaches.

Authorities can fine companies that fail to protect personal data as much as 2% of their global annual turnover or ¤10 million, whichever is higher. Given the scale of these fines, organisations may want to proactively protect certain categories of personal data.

Ab Initio software includes built-in capabilities for masking and encrypting personal information across all technologies, from mainframes to databases to Hadoop data lakes. Personal data can be protected across the enterprise based on business-term-driven rules. Data stewards and data owners can define protection schemes for either encrypting or tokenising data using a simple, intuitive user interface that does not require a programmer.

To create a protection scheme, a data steward simply needs to:

1. Identify which fields contain personal data (see the "Discover" section). An outcome of the discovery process is that the Ab Initio software captures metadata for the systems that hold personal data.
2. Create data protection rules by assigning business terms with a sensitivity level (High, Medium, Low).



	Name	Description	Sensitivity	Domain	Action	Generator	Arguments	AllowableCharsList
1	Bank Account	Bank account numbers	medium	global	encrypt	fpe	----+*-	numeric
2	Credit Card	Credit card numbers	high	global	tokenize	vaulted	----+*99	numeric
3	Debit Card	Debit card numbers	medium	global	encrypt	fpe		numeric

3. Designate a specific action and encryption for each term. For example, credit card numbers can be tokenised using the unique identifier generator.

TOKENISATION VS. ENCRYPTION
The terms encryption and tokenisation are often confused. Encryption replaces a value with another value by applying an algorithm to it, typically secured with a key. The original value can typically be retrieved by an appropriate decryption algorithm run by anyone with access to the key.

Conversely, tokenisation replaces the original value with a randomly assigned token — that is, not something generated by an algorithm, and, consequently, not something that can ever be programmatically decrypted. The association between a token and the original value is maintained in a vault, which is a secured datastore.

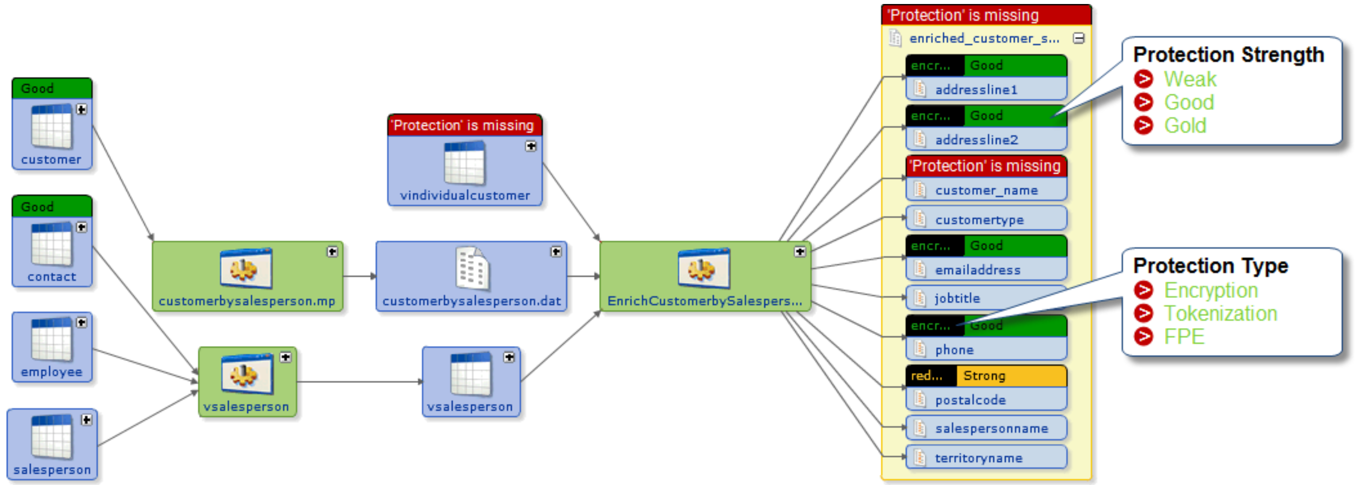
Tokenisation is generally accepted to be the strongest form of data protection.

Typically, protection schemes apply encryption, format preserving encryption (FPE), or tokenisation to all linked data elements. Each scheme, in turn, can be implemented by any number of "generators" — applications that apply the protection mechanism in a certain way. Data stewards can specify not only the type of encryption or action they want applied to the data, but also the scope of that application. Stewards can specify whether they want protection applied to all fields linked to a business term or just a specific field in a local dataset. Stewards can also specify how masked data is represented. It's possible, for example, to not only tokenise a credit card number, but also generate a token that itself is a valid card number.

Companies that do not want to encrypt all personal data may want to perform pseudonymisation on selected fields, such as on the unique identifier in each record.

Ab Initio's ability to perform format-preserving encryption or tokenisation on an individual field — based on business-term-driven rules — makes pseudonymisation possible.

When organisations use Ab Initio software to protect personal data, lineage diagrams show the protection status (whether a field is encrypted or tokenised) and rate the strength of the protection. The lineage shows a Red-Amber-Green overlay, clearly indicating the strength of protection for a given field, whether the strength is appropriate, or when data protection is missing.



This lineage diagram highlights missing data protection in red, with "Protection is missing." In this case, the field "customer_name" is missing protection. When a field's protection isn't sufficient for its associated business term's sensitivity category, the lineage diagram will also highlight this as a risk.

Ab Initio software controls which users are allowed to decrypt or detokenise data, how often, in what volume, and through which interfaces. If users do not have appropriate permissions, they will see data in its secured form. If users have appropriate permissions and are acting within their security remit, they can see the clear-text data.

Ab Initio software also provides a clear audit trail by logging all access requests and attempts to violate access policies, and by recording details of all data items that have been served.

PSEUDONYMISATION — A data processing technique that replaces one attribute — such as a unique identifier — in a record with another. This technique does not anonymise data, but it does reduce the linkability with the data subject's identity.

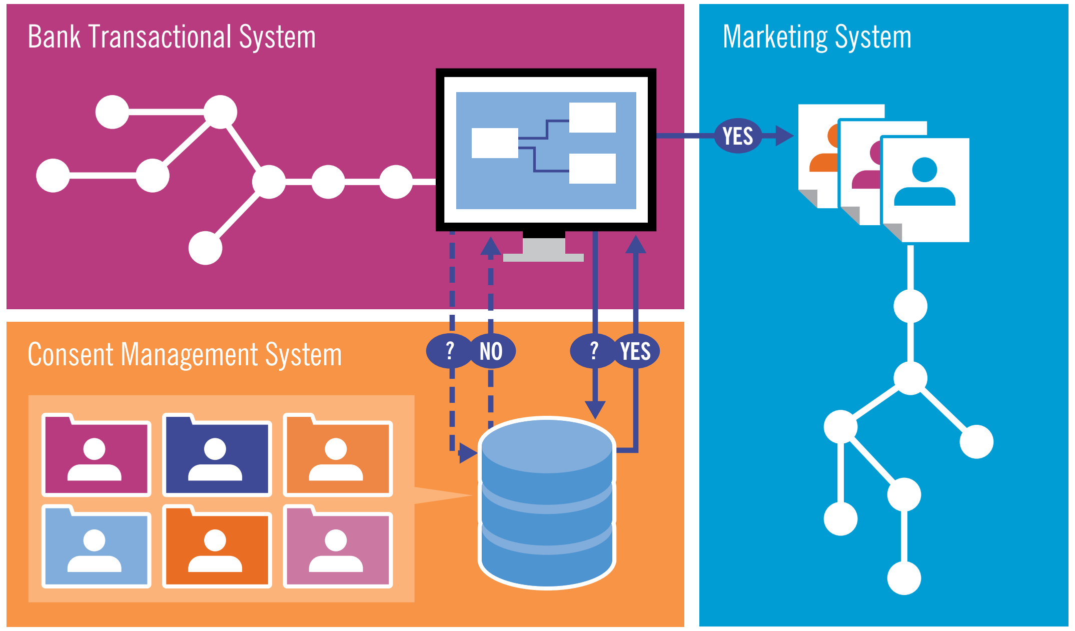
Typical pseudonymisation techniques include encryption with a secret key, hash functions, keyed-hash functions with stored keys, keyed-hash functions with deletion of the keys, and tokenisation.[9]

Consent-based Processing and Consent Management

Many organisations are concerned about maintaining consent-based processing. They fear that personal data could propagate into un-consented systems or proliferate unchecked throughout their organisation.

Organisations require robust consent management systems that are customised to their businesses and are extensible as requirements change. Such systems encode a data subject's consent choices.

The Ab Initio software enables organisations to create applications that check a data subject's consent encoding before allowing data to be processed, for example, by a Marketing system.

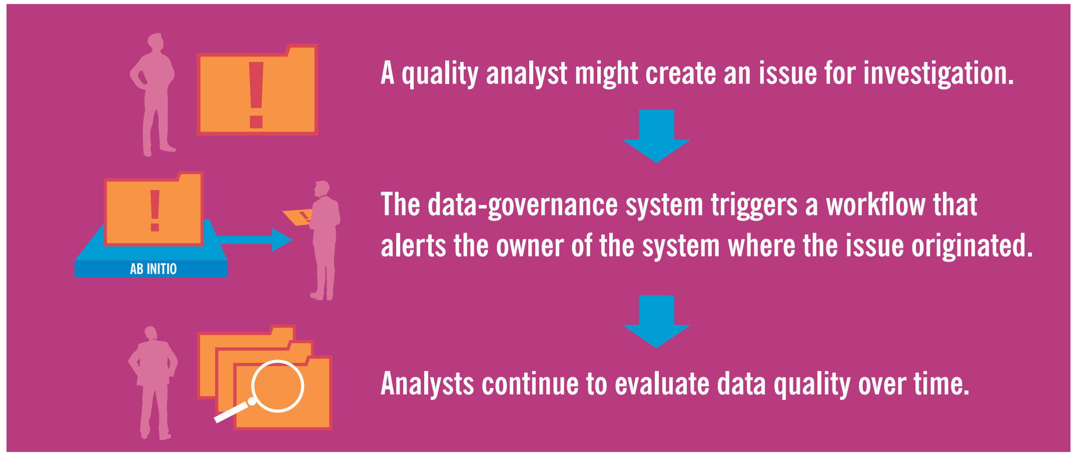


Ensuring Accuracy and Preventing Data Quality Issues

The GDPR stipulates that a subject's data must be accurate and, where necessary, kept up to date, and implies that companies need to take steps to ensure the accuracy, timeliness, and completeness of their personal data holdings.

Ensuring accuracy requires not only responding to complaints from data subjects about the correctness of their data, but also ensuring high data quality through the measurement of characteristics. Testing data's accuracy and completeness is an integral part of meeting the GDPR's accuracy principle. Ab Initio technology tests for completeness, accuracy, and timeliness and can even test data during real-time processing.

Workflow and issue management complement data quality checks, enabling organisations to create maintainable routines to ensure that they stay in compliance. For example, if data quality tests detect that 50% of postal codes do not match the city name in data subjects' addresses, the following human and automatic processes could take place:



A quality analyst might create an issue for investigation.

The data-governance system triggers a workflow that alerts the owner of the system where the issue originated.

Analysts continue to evaluate data quality over time.

If data quality problems are identified, they are always cheaper to fix at the source rather than downstream, after the data has been processed, transformed, or replicated in numerous systems.

Preventive, Detective, and Corrective Controls

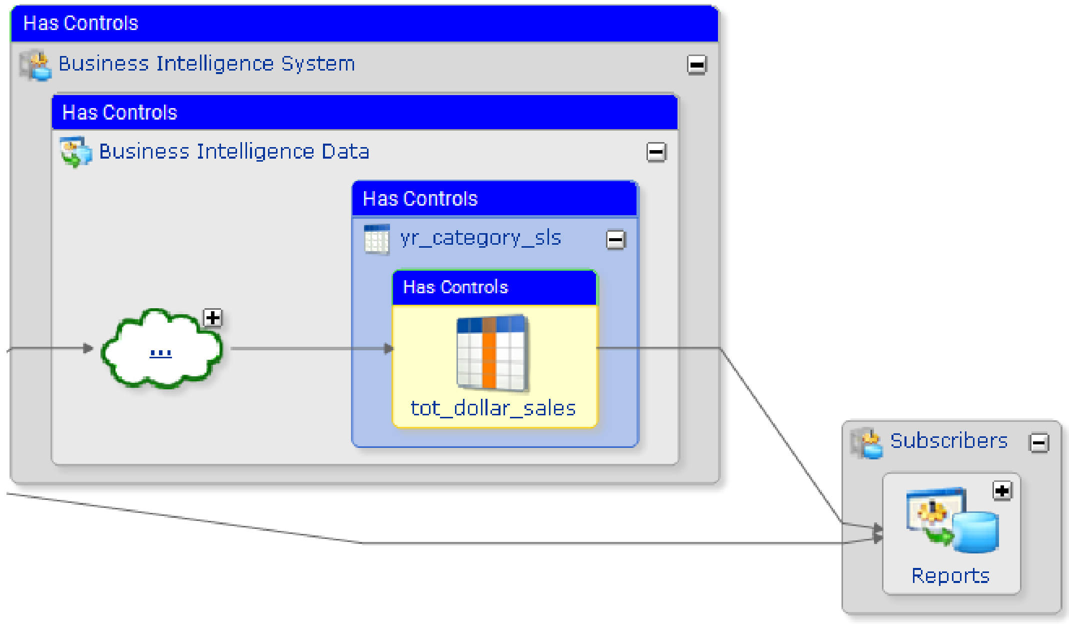
An integral aspect of ensuring quality is creating controls, which may in some cases prevent issues from occurring in the first place. Controls can be executable or manual processes to verify that a specific policy is functioning as it should.

Controls demonstrate to auditors that you have the mechanisms in place to ensure that you are meeting requirements. Because controls create a clear and auditable trail of actions associated with points of risk, auditors may want to review these controls and their associated analysis in the event of an investigation. Ab Initio software enables you to create executable controls and document manual processes (or enshrine them in a workflow).

Executable controls can be Ab Initio applications, business rules, or other executables that function as:

- **Preventive controls** — Processes designed to keep issues from occurring; for example, an application that prevents the Marketing system from obtaining unauthorised ("un-consented") personal data.
- **Detective controls** — Processes to determine whether issues exist; for example, a data quality process that detects whether unauthorised personal data is in the Marketing system.
- **Corrective controls** — Processes to remediate records with issues; for example, a corrective control (such as an application) that deletes or masks any unauthorised personal data that a detective control found in the Marketing system.

Ab Initio software allows you to see at a glance where controls are missing. The fields, datasets, and systems that have controls are shown in the data lineage as exemplified in the following screen capture:



Using Workflows for Issue Resolution and Routine Operational Tasks

Creating template-style, automated processes that guide data protection staff through routine tasks not only is more efficient than relying on manual checklists, but also creates documentation that demonstrates to regulators that you are consistently upholding GDPR principles.

The Ab Initio software supports the creation of such processes, enabling organisations to create workflows for:

- Performing Privacy Impact Assessments (PIAs) and approving the use of personal data in new systems
- Creating, collaboratively modifying, and approving new business terms for personal data
- Encrypting or tokenising new personal data in order to ensure its protection
- Remediating unauthorised use of personal data
- Fulfilling the "right to be forgotten"

Workflows can trigger applications and can also be integrated with web services.

Such workflows can be useful in a matrix-style GDPR environment, helping members of the Data Protection Office notify external team members that they need to remediate an issue. Because notification controls are extremely fine-grained, notifications can even be triggered by events — for example, an email could to be sent to your organisation's Security team based on a keyword such as "violation" in the text of an event.

CONTROL

Once your systems are catalogued, your data secured, and your environment brought into compliance, it's time to let the data-governance processes and controls that you've put in place do the hard work. At this point, the role of your Ab Initio data-governance system becomes one of "business as usual" — detecting when personal data has crept into your environment, guiding personnel through remediation requests, and monitoring the results of controls and other data quality tests.

Throughout, Ab Initio's metadata system can guide Data Protection Office personnel as they oversee Privacy Impact Assessments and interface with system architects, as well as perform audits and other reviews.

Manage Ongoing GDPR Issues

Effective GDPR programmes will cater to the day-to-day ongoing management of personal data protection policies, accountabilities, and tasks, ensuring that the organisation remains current in its usage of personal data. Ab Initio software enables organisations to successfully manage ongoing GDPR requirements by permitting them to:

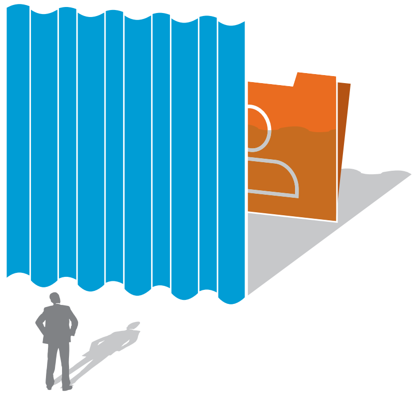
- **Capture issues** — Whether an issue arises during a regulatory audit, through a breach in data protection, in quality defects identified by a quality control, or in association with recurring processes, the Data Protection Office can properly capture the problem.
- **Monitor issue resolution** — Data Protection Officers can monitor issue-resolution assignments by employee and see who is assigned the most issues, where roadblocks exist to completing tasks, and the status of issues and remediation workflows. When issues aren't being resolved, Data Protection Officers have transparent insight through a detailed view of issues and how they are handled.
- **Create remediation plans for structural issues** — When an issue is complex, Ab Initio software enables Data Protection Officers to create a remediation plan to investigate the issue's root causes and manage its impacts.
- **Track compliance status** — Data Protection Officers can see a consolidated view of issues and goal status, which shows issue resolution rates and progress made.

Ab Initio software provides a central dashboard that enables Data Protection Officers to see GDPR issue status and how far they are from goal completion.

Running Privacy Impact Assessments

Under the GDPR, when an organisation embarks on the creation of a new system that processes personal data, the Data Privacy Office must perform a Privacy Impact Assessment — an evaluation of data subjects' risk from such processing — and review of how the system design will comply with GDPR principles.

The Data Privacy Office should document the following during Privacy Impact Assessments:



- The manner in which the system is intended to process personal data, and the purpose
- Which personal data the system will process and who will have access to it
- How long the information will be retained (and a justification for that time period)
- How processing could impact the rights and freedoms of data subjects (or their evaluation of how it does not)
- How the company will protect the personal data and mitigate any risks that have been identified
- The basis for processing the data (consent, lawful, etc.)
- Which third parties may have access to the personal data both in the EU and outside of it (that is, countries the EU Commission has designated as having sufficiently high protection levels)
- The Data Privacy Office's evaluation of whether it is necessary to contact the national data protection authority to oversee the Privacy Impact Assessment

When do you need to perform an impact assessment? Whenever your legal team indicates that you should, and quite possibly in the following situations:

- Whenever you create a new system in which automatic processing delivers information and forecasts or makes decisions or measurements based on certain categories of personal information (such as a person's race or ethnicity, religious or political affiliations, trade-union membership, health status, sexual orientation, economic situation, or criminal history)
- Whenever you create a new system that processes biometrics or genetic data, contains the data of children, or performs large-scale monitoring
- Whenever you implement a new system that processes personal data using a new technology

Other circumstances when you may need to perform a Privacy Impact Assessment include during mergers or acquisitions; at the time of international data transfers, system conversions, or database modifications; or when entering new vendor relationships.

Given the breadth of situations that may necessitate a Privacy Impact Assessment, it's essential that organisations have an efficient, repeatable process for performing such evaluations. Ab Initio software provides general workflow functionality, which organisations can customise to facilitate Privacy Impact Assessments, creating an orderly, methodical process in which nothing is forgotten. At the same time, Ab Initio's data-governance technology automatically documents actions performed via workflow, which, in turn, enables the Data Protection Office to quickly assess records in the event of an audit.

Subject Access Requests (SARs)

Under the GDPR, data subjects — including employees and customers — can submit Subject Access Requests (SARs) to request information about the personal data the organisation holds about them, including a copy of that data.

When organisations fulfil SARs, they also must disclose their data-processing objectives and disclose any third parties that received a subject's data. Organisations must provide this information in clear, concise language that the data subject can understand.

The GDPR stipulates that organisations must fulfil SARs within one month. For organisations in countries that have enjoyed lengthier response times for SARs — or do not have a prescribed time frame for response — this shortened window may prove challenging, especially for organisations lacking automated processes to handle SARs.

Under the GDPR, data subjects can request the following information:

- The purpose of the data processing
- The categories of personal data stored
- The storage location of the data (a potentially problematic requirement for cloud architectures), which also includes any other countries where the data has been or will be disclosed
- The length of the data retention period
- The source of the data and any other available information, if the subject did not provide the data directly to the controller
- Any automated decision-making processes, such as data profiling, and information about the logic of those processes and its consequences[10]

After data subjects review their personal data, they can request corrections to that data. Subjects can also withdraw their consent and request restrictions on their personal data.

The satisfaction of these requirements can be handled in two parts:

1. Describing in plain language the requested characteristics of data or its usage
2. Providing a verbatim copy of the data as processed

Searching for an individual data subject's personal data requires:

- Creating federated queries of all the systems where that person's data might be stored.
- Having a means to perform subject selection — Is this person actually the person whose data we've retrieved?
- Protecting sensitive information — such as national identification numbers, passwords, or credit card numbers — from all but a select group of authorised users.
- Being able to perform the queries quickly.
- Being able to limit the scope of the systems searched — personnel performing these searches should not be able to search for similar information in HR systems, for example.

SARs may require the description of the characteristics of data and data usage, and these can be obtained from the data-governance information that is captured by Ab Initio software. For example, the Ab Initio business lineage succinctly depicts data usages — and this information can be automatically exported to systems fulfilling a SAR (for example, to shape the query).

Ab Initio software enables organisations to support many of the requirements involved in satisfying SARs. For hierarchical data that cannot be queried with SQL, it's possible to build Ab Initio-based applications that query hierarchical data behind the scenes.

The Right To Be Forgotten

Perhaps one of the most problematic aspects of the GDPR is a data subject's "right to be forgotten" (right to erasure). A data subject can request that an organisation delete his or her data.

What will companies do when they receive requests to erase a subject's data? How can they be sure that a record does indeed belong to the same person who made the request? How can they then demonstrate that the data has been erased?

Systems that help companies comply with the "right to be forgotten" must account for all of the following:

- The need to perform different actions — such as deleting data or rendering it un-processable — based on the purpose of the system holding a given record:
  - Companies need to validate that any automated deletion of personal data won't corrupt the system where the data resides.
  - Generally, personal data associated with commercial transactions must be rendered un-processable in a reversible way for tax and audit reasons. However, companies may choose to delete personal data in other stores, such as Marketing systems.
- The need to have the appropriate permissions for all systems that store personal data. Any "right to be forgotten" solution that systematically deletes personal data must act only in response to proper authorisation.
- Companies need to establish a paper trail of "right to be forgotten" requests, and the resulting actions taken, for audit purposes.

Ab Initio software can also help with "right to be forgotten" requirements. First, Ab Initio software can provide clear insight into where personal data is held, including the systems and technologies. Second, Ab Initio software provides a flexible classification model that can be used to classify personal data systems by their "right to be forgotten" requirements; for instance, you might tag one system as "Delete data" and another as "Render data un-processable." Finally, Ab Initio's workflow functionality can be used to initiate and manage the process of effecting a "right to be forgotten" request.

Beyond this, Ab Initio software can also be used to rapidly construct applications to seek personal data and implement erasure policies as desired.

Data Portability

The GDPR provides data subjects with the right to move their data to another data provider. The GDPR dictates that organisations must provide a subject's data to that individual, upon request, in easy-to-understand language as well as in a standard, portable format the subject can take to another data provider — or use at home.

The second requirement may seem baffling at first. The ability to use personal data at home — or, as the GDPR puts it, the right to store data for "further personal use on a private device" — has many use cases, ranging from downloading purchase histories from a grocery store's loyalty card to obtaining health information from a fitness app. A newly married couple might even want to download a copy of their wedding registry — after the wedding takes place — so, as they pen their thank you notes, they have a list of which gifts their guests purchased.

Data portability solutions must be sufficiently flexible that they can meet the following requirements:

- The data subject has the right to transfer data about him- or herself. This includes third-party data and pseudonymised data that can be clearly linked to the data subject. This also includes information the data subject knowingly provided and data your organisation has observed or otherwise captured (search history, location data, age, or inferences about behaviour).
- The data must be available in a format that enables it to be used on a private device. Examples of data that subjects might want to retrieve include the contact information from webmail applications or playlists from music-streaming services.
- Data subjects can request both the data that they provided to your company as well as data that you have derived or inferred about them for analytical purposes. Examples of inferred data include things such as credit scores, or the outcome of health assessments. (You do not necessarily need to provide inferred data unless a data subject explicitly requests it.) As a result, you will likely want your data portability system to have the ability to distinguish between different types of data for a data subject and generate either one of these sets of data upon request.

Ab Initio software can be used to build applications that connect to all of the places where personal data is stored in your environment — whether it be Hadoop, relational databases, or mainframes — converting it to the requisite data format and packaging it securely for transmission.

Which Personal Data Can Be Transmitted

The provision for data portability doesn't mean that you simply give data subjects a dump of whatever data you possess about them.

Companies need to be careful that they don't transmit data to the new data controller that could affect the rights of third parties associated with the data subject; the names of people who wired money into the data subject's bank account, for example, may not be used for marketing purposes.

Article 29 states that data controllers should implement tools that let data subjects select the data that they want included in and excluded from the transmission to their new data controller. Presumably, this implies, at a minimum, a method of displaying information about the categories of data that you possess on a person.

In some cases, data controllers may also need to create mechanisms for requesting consent from third parties whose names or personal information appear in a subject's data.

Your Company May Need to Consume Data from New Customers

When new customers want to bring personal data to your company — whether it's from a competitor or a complementary service in your ecosystem — you will need a system that enables you to receive and ingest this personal data:

- This system must be able to submit a request, on behalf of your new customer, for the transfer of his or her data. You (or your web portal) must clearly explain to the customer the purpose of the data processing before you make the request and obtain his or her active consent.
- Once your system has obtained this consent, it must be able to send a request for the transmission of portable data to the other data controller.
- The request mechanism must contain a means for your new customer to select which types of data he or she agrees to transfer.

Furthermore, because a data portability request doesn't automatically imply data erasure — but subjects can request erasure — the system must be able to erase data upon request. In some cases, the data subject may still want to do business with you — such as a bank's customer who wants to transfer financial data to a budgeting service.

Once you receive the subject's data, certain precautions need to be taken into account as you ingest it:

- You can't process information for marketing purposes about anyone other than the data subject. If the subject's contacts have indirectly been disclosed (and those contacts haven't provided consent), you may need to identify and redact their information. An example of this might be a third party's contact information from a wired money transfer.
- You should not keep any data that is not relevant to the consented purpose of the new processing. Budgeting services, for example, do not need to keep all information they receive from banks beyond that what they require to create the budget. [11]

Data Portability Format

Data subjects can request that you transfer their data directly to one of your competitors. This raises a variety of issues:

- The GDPR does not specify the format in which companies should provide data. Rather, it encourages cooperation between industry stakeholders. What happens, however, when technology evolves and stakeholders decide on a different format?
- How do you provide your customers with data from loyalty cards or what their guests have purchased from wedding registries, in a format they can use on their own personal computers?

When you package a subject's personal data, the GDPR dictates that you must provide as much metadata as possible, at the deepest level of granularity, so as to preserve the data's meaning. If you do not do so, you risk violating the data subject's right to re-use the data.[12]

In some situations, systems packaging data for portability also may need to provide controllers with a choice of formats. (In this case, formats that lack such metadata must be made clear to the subject.)

Data Portability and Security

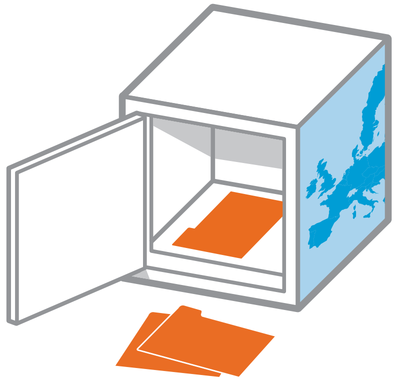
The GDPR focuses on the security of personal data, so it's not surprising that this also applies to the transmission of personal data for portability purposes:

- Systems for data portability must ensure that the data subject requesting the data is indeed the subject in question and that data will arrive at the correct destination. This will likely entail some form of authentication.
- Data packages must be transmitted securely (encrypted). Although the GDPR does not explicitly state that the contents of packages must be encrypted — in fact, it implies they might not be in some cases — data controllers need to consider how the receiver will handle the data. Data that is manually received may need to be masked in a reversible way to prevent personnel at the receiving organisation from seeing it.

The Ab Initio software enables you to build applications that provide automated mechanisms to meet data portability requests and ingest data that new customers have transferred to you. At the heart of this is Ab Initio's Co>Operating System software, which enables applications to connect to and process data from almost any data source in virtually any format, and to apply any level and type of data transformation necessary to map your data into a portable format, and to map data you receive into formats that your systems can understand.

Breach Notification Management

In the two years leading up to the GDPR's ratification, data breaches in the financial-services sector rose by an alarming 183%.[13] And some hacked companies were less than forthcoming, or were slow to warn customers that their personal data had been compromised. Perhaps it shouldn't be any surprise that the GDPR has chosen to encode strict requirements not just for protecting data but also for communicating when breaches occur.



Organisations must notify data subjects within 72 hours of a breach — the only exception is if the organisation encrypted or otherwise rendered the personal data unintelligible.[14] (Even then, organisations must still notify the supervisory authority that a breach occurred, and do so within 72 hours.[15]) GDPR introduces two levels of notification for data breaches:

- **Only notify the data protection authority** — Organisations must notify the data protection authority of any security incidents that affect the integrity, confidentiality, or security of their employee and customer personal data.
- **Notify your customer** — Organisations must notify the affected data subjects within 72 hours if the compromised data can result in discrimination, identity theft or fraud, financial loss, damage to reputation, or other significant economic or social disadvantages.

For organisations with ungoverned personal data usage, this 72-hour notification window will likely make compliance challenging.

Should a breach occur, it's important that you be able to meet the GDPR's stringent reporting and notification requirements. Avoiding fines isn't the only driver for communicating clearly after being hacked. Effectively communicating with data subjects helps organisations reduce reputational damage.

A 2014 Deloitte consumer product and executive survey revealed that 51% of consumers would forgive a consumer product company that had one single breach of its personal data — provided the company quickly addressed the issue.[16] While this statistic isn't particularly heartening, it does imply this: If you experience a breach and you hope to keep your customers' goodwill, you should contact the affected customers immediately and explain your remediation plans.

When organisations have already built Subject Access Request solutions using Ab Initio software, it may not be difficult to create a variant of this work so as to generate a list of data subjects affected by the breach. Such a list could include the specific data compromised for each person and the processing purpose of the breached systems. Creating a breach notification system is the type of proactive preparation that helps reassure regulators that your organisation has a breach response plan.

Even without such a system, Ab Initio's data lineage feature enables organisations to rapidly view their personal data storage locations across the enterprise. Quickly seeing which specific systems contain what personal data enables organisations to understand the extent of a breach and what data may have been compromised. Other Ab Initio software capabilities include data-search techniques, powered by federated queries, that enable organisations to quickly retrieve records of interest from affected systems.

It's possible to proactively create a "breach overlay" for lineage, showing at a glance the sensitivity of the compromised systems. Did the hackers attack systems containing personal data? Credit card numbers? Trade secrets? Contracts? This is the type of information organisations will want in the event of an attack or breach, in order to determine the impact.

Final Thoughts

For organisations that need to comply with the GDPR, Ab Initio software can provide a highly flexible and effective way to support organisations' GDPR compliance requirements and to keep them current. Ab Initio enables organisations to build and configure the functionality they need in order to meet their individualized requirements.

The data-governance aspects of the Ab Initio platform enable organisations to formulate their GDPR data- governance policies, procedures, and controls, to allocate and manage accountabilities, and to identify the location of personal data and track its processing (that is, what was done and under what rules) throughout their systems. Data-protection policies driven by business rules make it easier for data stewards to protect personal data — whether it is just for one or two identifying fields per dataset or across all personal data in the enterprise. Of course, GDPR compliance is a complex subject; while Ab Initio can provide powerful tools, achieving compliance will require involvement of many types of expertise and ultimately will require your reliance on expert legal counsel (not Ab Initio) to interpret the regulations and determine your organisation's risk tolerance.

For organisations that want to create new systems or frameworks of business rules, or to conduct consent-based processing, Ab Initio's innovative technologies dramatically reduce development time and, in many cases, return business rule development to the hands of business analysts rather than developers. Many of the world's largest organisations rely on Ab Initio software for data governance, data integration, and decision-making with transparent auditability.

Please contact Ab Initio today to learn more about Ab Initio's position on GDPR and a demonstration of our capabilities.

[1] European Parliament. Data protection reform - Parliament approves new rules fit for the digital era. [Luxembourg]: European Parliament News; 2016 Apr 14 [accessed 2017 Mar 20]. Plenary Session Press Release. http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era

[2] Carson, Angelique. ICO's Wood: GDPR grace period? No way. Portsmouth (NH): IAPP; 2017 Mar 15 [accessed 2017 May 16]. https://iapp.org/news/a/icos-wood-gdpr-grace-period-no-way/

[3] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 Apr 4]; L(119):33.Article 4,1. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[4] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 Mar 10]; L(119):11.I,58. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[5] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 Jun 6]; L(119):35.Article 5. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[6] Goel V, Perlroth N. Yahoo Says 1 Billion User Accounts Were Hacked. New York: New York Times; 2016 Dec 14 [accessed 2017 Mar 31]. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

[7] Tanner, Adam. How A ZIP Code Can Tell A Marketer Exactly Who You Are. New York: Forbes; 2013 Jul 22 [accessed 2017 Mar 16]. https://www.forbes.com/sites/adamtanner/2013/07/22/how-just-a-zip-code-can-tell-a-marketer-exactly-who-you-are/#27b8639a426a

[8] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 May 31]; L(119):35.Article 5,1c. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[9] European Commission. Article 29: Opinion 05/2014 on Anonymisation Techniques. Brussels: European Commission; 2014 Apr 14 [accessed 2017 May 21]:20. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[10] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 May 20];L(119):43.Article 15. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[11] European Commission. Article 29: Guidelines on the right to data portability. Brussels: European Commission; 2016 Dec 13 [accessed 2017 May 20]:6. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

[12] European Commission. Article 29: Guidelines on the right to data portability. Brussels: European Commission; 2016 Dec 13 [accessed 2017 May 20]:14. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

[13] Ashford, Warwick. Financial sector data protection breaches up 183% in past two years. Newton (MA): ComputerWeekly.com; 2015 Jun 3 [accessed 2017 Mar 28]. http://www.computerweekly.com/news/4500247427/Financial-sector-data-protection-breaches-up-183-in-past-two-years

[14] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 Mar 21];L(119):53.Article 34,3a. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[15] European Commission. Regulations. Official Journal of the European Union. Brussels: European Commission; 2016 May 4 [accessed 2017 May 11];L(119):16-17.I,85. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[16] Conroy P, Narula A, Milano F, Singhal R. Building consumer trust, Protecting personal data in the consumer product industry. Westlake (TX): Deloitte University Press; 2014 Nov 13 [accessed 2017 Jun 4]. https://dupress.deloitte.com/dup-us-en/topics/risk-management/consumer-data-privacy-strategies.html

ABOUT AB INITIO

Ab Initio is a global software company headquartered in Lexington, Massachusetts. For more than 20 years, Ab Initio has worked with the largest and most sophisticated organizations in financial services, telecommunications, healthcare, retail, high-tech, transportation, manufacturing, and government, among others, to assure their business success.

Ab Initio products are designed, from the beginning, to provide a single, cohesive technology platform for scalable, high performance data processing, integration, and governance.

Ab Initio software is transforming the way large institutions manage and process their data.

To find out how Ab Initio can help you meet GDPR requirements, contact us: solutions@abinitio.com

CORPORATE HEADQUARTERS
Ab Initio
201 Spring Street
Lexington, MA USA 02421
+1 781-301-2000 (phone)
+1 781-301-2001 (fax)

UNITED KINGDOM
3 The Heights
Brooklands
Weybridge
KT13 0NY
United Kingdom
+44 (0) 870-850-8700 (phone)
+44 (0) 870-850-8701 (fax)

FRANCE
1 rue Danton
75 006 Paris
France
+33 1-42-34-90-00 (phone)
+33 1-42-34-90-01 (fax)

GERMANY
Landsberger Strasse 302
80687 München
Germany
+49 89 90405-800 (phone)a
+49 89 90405-809 (fax)

POLAND
Aleje Jerozolimskie 96
00-807 Warsaw
Poland
+48 (22) 275-5744 (phone)
+44 (0) 870-850-8701 (fax)

TURKEY
Buyukdere Cad
No 173A Kat 7
Levent 34393
Istanbul
Turkey
+90 212 386 3277 (phone)
+90 212 386 3200 (fax)

JAPAN
The Imperial Hotel Tower 15/F
1-1-1 Uchisaiwaicho, Chiyoda-ku
Tokyo 100-0011
Japan
+81 3-3507-5734 (phone)
+81 3-3507-5601 (fax)

SINGAPORE
Level 21 Office N0. 3423
3 Temasek Avenue
Singapore, 039190
+65-6549-7906 (phone)

AUSTRALIA
Level 20 Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000
Australia
+61 448 591 253 (phone)

Ab Initio