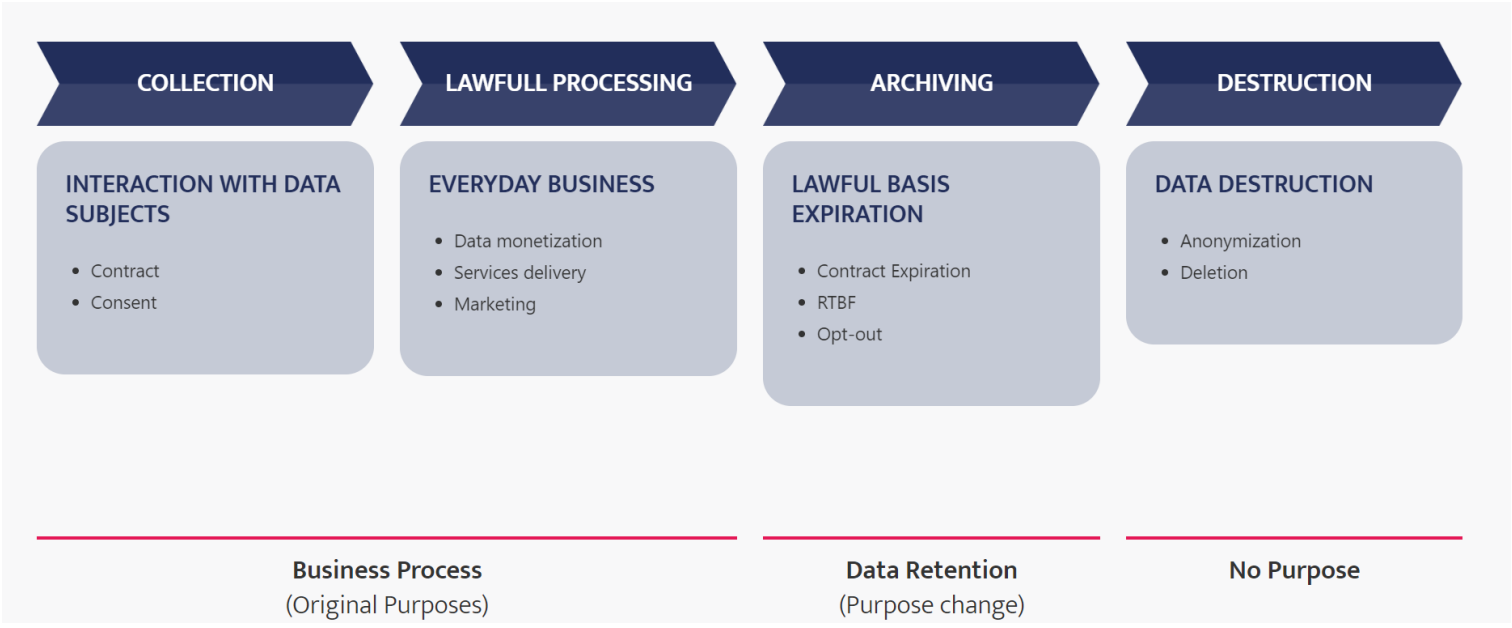
Comprehensive privacy solution for effective personal data management

Data Privacy Manager is a globally recognizable privacy management platform used in many different vertical markets. It helps Companies, both data controllers and data processors, be trusted and accountable. The platform design enables privacy process centralization, and full control over personal data processing lifecycle, from data collection until data removal from all systems.

Data Privacy Manager empowers companies to simply manage privacy risks, individual's rights, and their preferences. By protecting individual's privacy, Companies are minimizing regulatory risks and building the image of a trusted brand.

CENTRAL MANAGEMENT AND CONNECTIVITY WITH OTHER SYSTEMS	COLLABORATION THROUGH ALL ORGANIZATIONAL UNITS	AUTOMATED DATA REMOVAL ORCHESTRATION
Central management of GDPR processes is enabled by connecting the Data Privacy Manager to all systems and applications that contain personal data.	Facilitates collaboration between Privacy, Technology, HR and Marketing. Promotes collaboration and de-centralized privacy governance.	Automated orchestration of data reduction in connected systems. Includes granular configuration of data retention policies and automated calculation of data removal schedule.

Data Privacy Manager is designed to support the organization's **Personal Data Lifecycle**



Data Privacy Manager is a modular solution comprised of **10 modules** designed to solve the most difficult privacy challenges:

Data Processing Inventory - Harbor cooperation between Privacy, Technology, and Business. Promote their collaboration and centralize information about data processing. Enable your team to work together towards compliance.

Third Party Management - Centrally manage Third Parties and guide your partners trough vendor management process workflow.

Data Subjects Request - Turn data subjects request into an automated workflow with a clear insight into data every step of the way!

Risk Management – manage risk assesments and privacy risks for personal data processing, systems and Third Parties.

Consent and Preference Management - Consolidate collected consents and preferences, enable Omni-channel Customer journey, manage Third-party data sharing, and promote transparent and accountable consent management.

Privacy Portal – Enable out-of-the-box self-service privacy management for your Customers. By giving them the control, you gain their trust!

Data Inventory – Build a central data register of discovered personal data across multiple systems in the cloud or on-premises.

Data Flow - Establish a business and operational control over complete personal Data Flow within your organization

Data Removal – Automate Data removal orchestration; Use Data Privacy Manager to automate the removal of personal data once you loose legal or business justification for processing.

Privacy 360° - Build a Privacy 360° view of the Data Subject. Understand WHY and HOW you are processing Data Subject's personal data, and create links to your operational systems.

Product modules description

Records Of Processing Activities

Challenge:

Keeping a compliant Records of Processing Activities imposes a serious set of challenges that leave companies disheartened, overwhelmed and often delaying the project awaiting the proper solution. The main organizational challenge is lack of cooperation between Data Protection Officer, Legal Services, IT, HR and Marketing, which is understandable given the complexity of the project and the variety of functions and departments involved. However, without cooperation, there is no division of responsibilities between departments, which means a DPO should possess both technical expertise in order to implement compliance policies and an understanding of the data protection laws.

The reality is that the DPO is usually an IT professional or legal expert, not both. Even if there would be a DPO who embodied both expertise, it is almost impossible for one person to have continuous insight into the regulatory segment and the data segment of all the business processes of the company, and the larger the scale the more impossible it gets.

The next challenge is of technical nature and is related to the technical execution of keeping the Records of Processing Activities.

The Records represents one of the main compliance pillars, giving the company an overview of procedures and significant information about data processing. Still, the record is usually kept in Excel, which does not offer collaboration function and a DPO can not track changes made in the document.

Moreover, it is impossible to administer other applicable laws or define data retention policies for each data category, because Excel does not allow you to execute those policies directly onto the appropriate data sets.

These challenges do not allow the company to move forward with the compliance project. If there is no division of responsibility between DPO and other organizational units, the DPO will be faced with the impossible challenge of overseeing all company processes.

On the other hand, if the company has recognized the importance of decentralized data privacy management model and there is a department collaboration but there is no proper

tool for managing the processes, the DPO will be left without an overview of all processing activities and unable to track changes made by other departments.

Solution:

Data Privacy Manager facilitates collaboration between DPO, Legal service, IT, HR and Marketing, allowing them to create clearly defined responsibilities that are realistic and consistent with the competencies of each organizational unit.

Division of responsibilities means that a DPO has a continuous insight into the legal regulatory segment and the data segment of all business processes of the company, advising Marketing and HR during the compliance process, while IT is resolved from in-depth understanding of data protection law and focused on the implementation of the policies.

Data Protection Officer has access to all processing activities and any changes to them, while other roles can create, edit and (de)activate processing activities. Each processing activity has its owner which indicates who is responsible for updating information related to processing. These functionalities of Data Privacy Manager make the Excel obsolete. The decentralized data privacy management model seals the DPO as a supervisory and advisory role, while IT, Marketing, HR and other departments take responsibility for their part of the compliance process.

This makes automatization of the entire personal data lifecycle possible, which is the only way to be truly compliant considering the amount of data that is being processed, the number of IT systems that process data, and represents the bases for automatization of all further compliance processes.

Benefits:

COLLABORATION	DIVISION OF RESPONSIBILITY	INTEGRATION WITH DATA PROCESSING SYSTEMS
Facilitates cooperation between DPO, Legal service, It and Marketing, allowing them to divide their responsibilities, making it possible for each organizational unit to create clearly defined responsibilities	DPO has access to all processing activities and any changes to them, while other roles can create, edit, and (de)activate processing activities. Each processing activity has its owner in Data Privacy Manager	Data Privacy Manager takes into account different business processes of the company and IT systems where data is processed, creating and propagating the archiving schedule and the data destruction policy with the technical data location information.

Third Party Management

Challenge:

Running a business today is unimaginable without vendors, partners, regulators, and other Third parties. Third parties can provide professional services and products, which help you bring additional value to your customers. In this relationship, personal data exchange is almost inevitable.

In terms of Data protection, sharing customer personal data is a risk which the Organization needs to mitigate appropriately. Sharing personal data with Third-party needs to be lawful and monitored. The challenge is to keep track of all Third-party data processing, their lawful basis and contracts, and inherent privacy risks. The Organization must manage its partners and vendors and ensure all personal data processing done by the Third-party is done responsibly and concerning data subjects' rights.

Data controllers hold the majority of responsibility in this relationship because they define the purpose of the processing activity and have control over the data. GDPR also states that the controller will only collaborate with processors that provide sufficient guarantees for implementing appropriate technical and organizational measures.

The data controller is responsible for choosing GDPR compliant data processor or risk penalties. So how to remain in control over data processing activities and make sure your data processor is a trustworthy partner?

Solution:

The goal is to have a controlled process of personal data sharing, enabled by legal and technical measures ensuring that the third-party vendor is acting in a GDPR compliant way. Data Privacy Manager helps companies to better understand the data disclosure basis for each of the data processors. It includes understanding and defining applicable safeguards to prevent abuse or unlawful access or transfer of data.

Third-party vendor management is impossible without risk assessment and Data Protection Agreements management.

Engaging in a business relationship with a third-party vendor is not a single event. It is an active and lasting process in which Data Privacy Manager helps you with keeping records and statuses of onboarding or offboarding process.

Benefits:

LEGAL FRAMEWORK	DATA PROCESSING AGREEMENT MANAGEMENT	PROCESS WORKFLOW MANAGEMENT
Enables DPO to define Data Disclosure Basis and applicable safeguards for each Data Processor in one single place.	Smart notifications inform you about all important events regarding Data Processing Agreements.	Managing Data Processors in a process workflow having correct information about their current involvement statuses.

Data Subjects Request

Challenge:

Data Subject Requests are one of the most difficult areas to cover under the GDPR. Companies mostly struggle with data portability and right-to-be-forgotten.

Every one of the Data Subjects' rights has certain specifics and requires different workflows in order to register, process, fulfill and document data subject's request. All while keeping track of response time and assuming you can locate the data in the company's system.

Any violation of those rights provokes the highest penalties under the GDPR while the risk of a lousy reputation can affect companies' opportunity to build solid and trustworthy customer relationships.

The company is also obligated to communicate any rectification or erasure of personal data or restriction of the processing. Notification must be sent to the data subject without delay and within one month of the receipt of the request. That is a challenge!

Solution:

Data Privacy Manager is a platform for orchestration and management of data subject's rights. It automates the entire process so that the IT systems, on which the data is stored, can execute user requests timely and accurately.

The process becomes an automated workflow giving you clear insight every step of the way, from the registration of a user request, through the process of the request approval and data processing, to the notification of the user about the outcome of the request.

Most importantly, the Data Privacy Manager represents one central place for the supervision of requests and provides DPO with all necessary information for managing data subjects' requests within the limits of respond date.

Combined with Privacy Portal as a customer-facing channel it gives company flawless insight into communication preferences of data subjects, their preferred language of communication, and purpose of data processing, while data subjects can opt- out as easily as they opted-in.

Benefits:

AUTOMATION	A CENTRAL REQUEST MANAGEMENT	TIMELY AND ACCURATELY EXECUTE USER REQUESTS
Automate the entire process with Data Privacy Manager, so that the IT systems, on which the data is stored, can execute user request timely and accurately.	Get a clear insight every step of the way, from the registration of a user request, through the request approval and data processing, to the notification of the user about the outcome of the request.	Execute data subjects requests within the GDPR time limit for responding to the request, which is no later than one calendar month.

Risk Management

Challenge:

Managing Data Subjects' data without proper risk management is putting every organization in a precarious position. In the case of GDPR, the risk we are identifying is not the risk for the organization, then the risk from the point of view of Data Subject.

Usually, there are three sources of risk.

The first is Third Parties – DPO needs to asses all Data Processors which have access or to which personal data is disclosed. It requires contractual protections with Data Processors and their Sub-Processors. Awareness what is the risk score of our Third Parties and acting to mitigate the risk is essential in avoiding the potential fines.

The second is IT (and non-IT) Systems, where personal data is stored. Organization needs to be aware of which kinds of security measures were undertaken. If it is a Cloud system, the location of the data center can affect the risk score.

The third source of risk is, of course, Data Privacy Impact Assessment (DPIA) which needs to be conducted when there is a systematic and extensive evaluation of the personal aspects of an individual, including profiling; or processing of sensitive data on a large scale; or systematic monitoring of public areas on a large scale. Out of DIPA, many risks can rise and we need to be able to properly manage them.

Solution:

Risk Management module of Data Privacy Manager module empowers your DPO with a high-level overview of risks associated with each processing activity; and to allow for a more detailed insight into residual risks behind a particular processing activity by means of linking it to a relevant data protection impact assessment.

Before assigning the risk to processing activity, third party or a system you will define the risk methodology your organization is currently using. It is possible to adjust the risk matrix both by impact and probability. As well, it is possible to define risk scores.

Having risk methodology in place and assigning risks to the key entities the solution creates a Risk Register, which acts as a guideline for the management. It shows where the organization is vulnerable and what should be the key next steps in order to provide compliant personal data processing.

DPIA register allows business process owners to download the DPIA template, to do assessments and upload the results back to Data Privacy Manager. By this organization is having all GDPR processes in one place.

Benefits:

CENTRALIZATION	CUSTOM RISK METHODOLOGY	DPIA REGISTER
Risk register and DPIA register is at the one place within the Data Privacy Manager together with other essential GDPR processes.	Adjust the risk methodology to the one your organization is already using and keep risk management comprehensive	Collaborate and create DPIAs, use available templates and upload the results.

Consent and Preference Management

Challenge:

New data protection regulations, including GDPR and e-Privacy, have challenged the landscape of direct marketing forever, introducing stricter standards on how consents are collected and the extensiveness of mandatory information that needs to be provided to the data subject prior to consenting.

The challenge is that the companies are lacking the insight into the personal data lifecycle and are unable to track, monitor and respond to the data subject's request and consents preferences.

The company's efforts to become compliant are futile if they do not know when to start or terminate data processing activity or how to demonstrate the compliance to the regulatory authority. The larger the scale the more operational challenges the company will face and having consents scattered across multiple channels makes this task complicated and needlessly difficult.

Solution:

Data Privacy Manager gives you real-time insight into the complete personal data lifecycle from the moment of opt-in to data removal. This creates a clear view of activities and enables you to demonstrate compliance for any data subject on any level at any point in time.

Consent and Preference Management module makes it possible to centrally manage notices and propagate them to all consent collection channels, automatically updating it across multiple marketing layers.

Companies using the Data Privacy Manager can give complete control of privacy preferences to the data subjects, giving them the possibility to set preferred communication channels so you can nurture the relationship through marketing activities on their terms.

This will give you the outlines of customer behavior and the opportunity to communicate your marketing messages never having to wonder if you are crossing the line.

Benefits:

SINGLE SOURCE OF TRUTH	SIMPLE DEMONSTRATION OF COMPLIANCE	EASY INTEGRATION
Data Privacy Manager serves you as a single source of truth for all collected consents. It allows you to timely start or terminates processing activities to ensure that all processing activities are GDPR compliant.	Provides real-time insight into the complete personal data lifecycle, from the moment of opt-in to the data removal. Create a clear view of activities and so you can demonstrate compliance for any data subject on any level at any time.	Easy integration with front-end consent collection channels like web, mobile apps, CRM systems, and marketing platforms, so you can automate every marketing action based on consent, making your actions transparent and compliant.

Privacy Portal

Challenge:

For some companies, data subjects' rights fulfillment is a restricting and overwhelming set of responsibilities and regulations. Other companies see GDPR as an opportunity to rethink their privacy model. They found an intelligent way to provide customers with truly important value – control over their personal data!

In order to comply with the principle of transparency, the company is obligated to provide appropriate information about the collection of personal data. Any communication relating to data processing should be delivered in a concise, transparent, and easily accessible form. Companies are also obligated to assure a straightforward and simple administration process of consent and preference choices..

Solution:

Companies with advanced maturity of privacy management introduced privacy portals as a way of giving customers control over managing their data and communication preferences. Some of them did not have an existing web portal or simply wanted to invest in a transparent relationship with their customers.

At the same time, they position themselves as businesses who are advanced-thinking, customer-oriented, and selling services or products, not personal data of their customers.

Privacy portal is a self-service interface for managing data subjects' privacy settings that allows

- Simple but highly secured access to their personal preferences
- Displayed all available consents with easy OPT-IN or OPT-OUT status change
- Available access to data subject's rights requests
- Information about the company's legal information like Privacy Policy and DPO information
- Unique hashed link for each Data Subject enables easy and secure access to Privacy Portal

Privacy Portal is a channel that helps you direct your communication at the right angle for each specific customer.

Having a privacy portal means having a tailor-made solution customized for the needs and visual identity of the company without the need for additional in-house development.

Benefits:

CONSENT MANAGEMENT	SIMPLE AND SECURE ACCESS	TAILOR-MADE
Straightforward Privacy Portal where customers can easily manage their consent OPT-IN and OPT-OUT status. It is automatically integrated with powerful Data Privacy Manager's consent engine.	Customers access Privacy Portal using automatically generated highly secured hashed link, unique for each Data Subject.	Get a tailor-made customer-facing channel that follows the visual identity of your company without additional in-house development.

Data Inventory

Challenge:

In order to manage personal data, companies first need to know where the data is stored. As business needs are growing, the number and complexity of IT systems are also growing. Before GDPR, there were no major concerns about personal data in those systems. However, things changed in many ways.

It is not uncommon for companies to have a low level of awareness about where they store personal data. This situation makes them incapable to fully address all requirements defined by GDPR.

Think about the situation where a company receives a request for the right-to-be-forgotten from a specific data subject. How can a DPO fulfill this request if there is no information about where exactly is personal data stored?

Understanding where data is stored within the company is a prerequisite to compliant data privacy strategy!

Solution:

The Data Inventory module connects to all relational databases of the company, making search inquiries, eliminating false positives and identifying all personal information across multiple systems.

This allows you to utilize the power of machine learning to precisely identify all personal data and to help you understand how data flows through your company.

Some of the companies tried to do a manual Data inventory, which resulted in exhausting a lot of resources and time with a questionable result. With manual data discovery, you can not be confident in results, and if a new system is added, you need to perform the whole task once again.

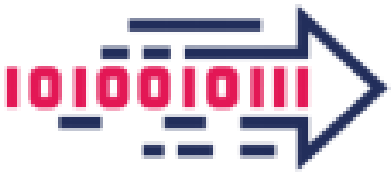
The Data Privacy Manager delivers an automatic Data Inventory process saving you time and enables companies to have a clear & correct starting point for the GDPR compliance project.

Benefits:

CREATE A DATA INVENTORY	ELIMINATE FALSE POSITIVES	TIME-SAVING
Highly precise identification of personal data across multiple company systems on-premise or in the cloud.	Prevent mistakes and errors in data reports and finally have accurate insight into the personal data.	Data Inventory module connects to the relational database and automatically delivers data discover result, so you can utilize your resources on other projects.

Data Flow

Challenge:



The compliance process begins when Data Inventory discovers all personal data stored across multiple companies IT systems. It is crucial to know where personal data is stored, but it is even more important to be aware of how an organization uses this data.

If there is no understanding of all 4 Personal Data Lifecycle components, addressing all GDPR requirements becomes very difficult. Collection of data and lawful processing are parts of original business purposes while archiving and destruction are tasks needed to perform once lawful basis expired.

Having an understanding of Personal Data Lifecycle in some chart or organigram is a good starting point, but nothing more. If a DPO does not have operational control over personal data, manual process management will soon become a highly risky and overwhelming task.

Solution:

The key to the Data Flow challenge is to use a professional tool, such as Data Privacy Manager which allows DPO to have the total control and overview of all personal data processes within an organization.

In the first phase of interaction with data subjects, which is part of the original business purpose, it covers all six lawful bases for personal data collection. Processing data for delivery of contracted services or marketing is the second stage and is also a part of original business purpose.

Once the contract expires or customer opts-out, the lawful basis for processing is no longer valid. This is when the archiving starts, which means the purpose of processing changed, and it triggers the data retention process.The last stage is the Data Removal phase in which an organization should no longer possess or process that personal information.

Data Privacy Manager is a unique solution with a variety of modules and workflows enabling Organization and a DPO to have control over Data Flow. Once when the

system is set up, processes are automated, and DPO can easily manage the personal data lifecycle.

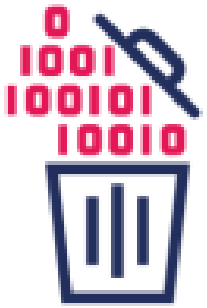
Benefits:

COMPREHENSIVENESS	BUSINESS PURPOSE MANAGEMENT	DATA RETENTION AND DATA DESTRUCTION MANAGEMENT
Data Privacy Manager brings organization comprehensive solution for complete Data Flow management	Automatically manage processes related to the original business purpose for both collection, and processing of personal data.	After the original business purpose expired Data Privacy Manager helps you manage Data Retention and Data Destruction processes.

Data Removal

Challenge:

Each personal data collected by the company goes through a personal data lifecycle. Data is collected through different channels, processed for everyday business operations. After the lawful basis for processing expires, personal data has to be archived for legal and documentation purposes and eventually removed.



The data removal process imposed a new set of challenges, amplified with the lack of understanding about where the data is stored, and no real insight into the technical and business implication of data removal.

At the same time, companies are expected to demonstrate compliance with fair information practice principles, storage limitation principle and the right to be forgotten. And with the laws that regulate documentation retention periods, like archiving law.

It gets more complicated when the data subject uses more than one active service of the company for which, very often, the same data sets are required on the same systems. For this reason, the data removal system needs to be intelligent enough not to erase the personal data that are still in use.

The last challenge refers to the technical orchestration of data removal. Since it is almost impossible to delete data in big enterprise systems, the GDPR recommends data anonymization and pseudonymization as opposed to deleting data. In the event of data deletion by mistake, there is a technical possibility of recovering data.

Solution:

When a company is processing a large amount of data across multiple systems, automation is the only way to avoid the possibility of human error and reduce the risk of non-compliance. Automation minimizes the amount of manual work needed for data deletion or to record every action taken over data.

Data Privacy Manager automatically gives instructions to a different system when data deletion needs to be executed and enables you to define data retention and data removal operationalization on different data categories.

Data Privacy Manager's automated services answer two key questions: "WHICH data subject's data needs to be removed?" and "WHEN this data needs be removed"?

Data retention schedule and Data destruction schedule are 2 real-time services available for end-to-end automation of personal data removal.This represents a GDPR compliant personal data removal engine.

Benefits:

AUTOMATION	DATA RETENTION SCHEDULE	DATA DESTRUCTION SCHEDULE
Privacy professionals do not have to spend their time giving instructions to the IT team on which data should be removed and when.	Precise real-time service keeping records and counting data retention period for personal data down to a single data subject level.	Automatically give instructions to different systems on which data should be removed and when.

Privacy 360°

Challenge:

As the compliance process continues, the Data Protection Officer faces specific challenges that are preventing the company from going forth with the envisioned data privacy model.

It becomes more and more apparent that there is a need for a clear understanding of data processing activities for each data subject across all company systems.

If you collect different sets of data from the same individual for different purposes, it can create different data sets for the same data subject in different systems. This causes you to have only a partial insight into what data is processed for that specific individual.

Lack of 360 overviews of personal data disables DPO from efficiently performing everyday tasks like fulfilling the right-to-be-forgotten or Data Removal. It puts a company in a highly risky situation since some data can be unintentionally left undeleted in the systems.

Solution:

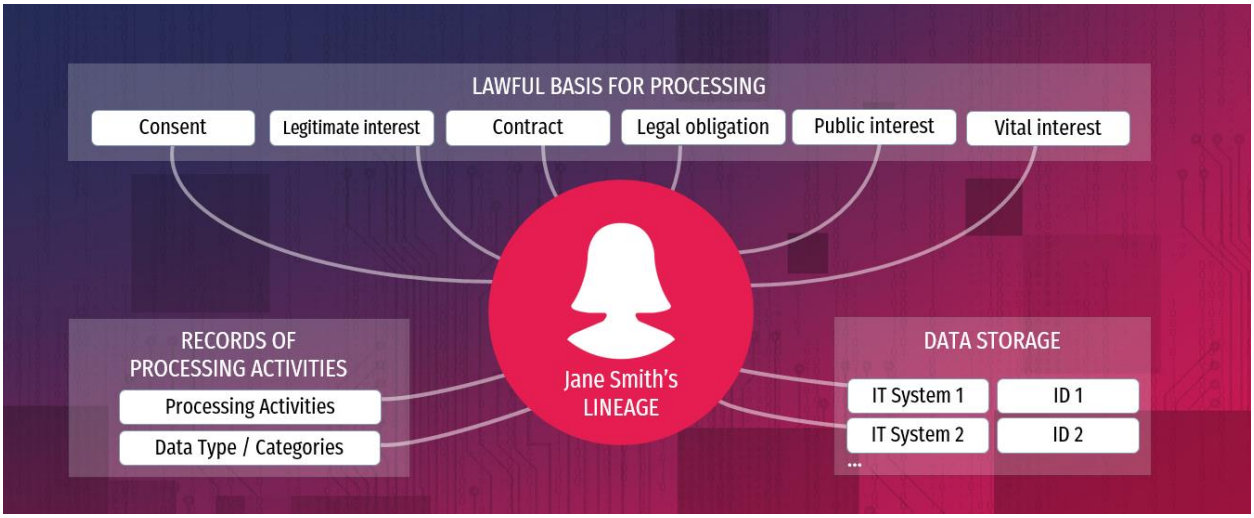
Privacy 360 is a reporting module and a perfect solution for the Data Protection Officer's challenges. It gives a DPO an overview of all data and locations where personal information is stored about the specific data subject. Privacy 360 answers the questions: what data is collected, how the data is processed and where is data stored?

Data Privacy Manager uses unique Identifiers (IDs) from each IT system containing personal data. Having information about all IDs from different IT systems regarding one single Data Subject is of the essential value to every DPO. This enables DPOs to perform GDPR tasks with confidence, having the correct information about all Data Subjects' data.

Based on input information a DPO can keep records of the master data subject with the help of recommendation engine, built-in data quality rules and, data merger engine. Combining Privacy 360 with the Privacy portal will give data subject an insight into how his or her data is processed so they can have control over their data every step of the way.

Benefits:

DPO REPORTING TOOL	360 VIEW	INSTANT INFORMATION
Reporting module created with your everyday challenges in mind.	It gives you an overview of all the data and information that belong to a specific data subject.	Get a comprehensive and instant view of data processing with full control over all processing activities.



www.dataprivacymanager.net