GENERAL DATA PROTECTION REGULATION & CUSTOMER IAM

CONSIDERATIONS FOR GDPR COMPLIANT SERVICES

WHITE PAPER

UBISECURE™

Connecting Identity.
Transforming Digital Business.

INTRODUCTION

The European Union's General Data Protection Regulation (GDPR) is globally the most substantial privacy legislation. As opposed to Directives, which will be implemented by each member state in turn, it is a regulation and is already in effect in all European member states, but not enforced until May 2018. All organisations handling any personal data of EU citizens need to comply with the GDPR, no matter where they are domiciled.

The requirements set forth by the GDPR are strict. Some of the requirements can be met with processes, while others are easier to implement with the help of technology. As the regulation deals with Personally Identifiable Information (PII), Identity and Access Management solutions can help in many areas.

Traditionally Identity and Access Management (IAM) has been associated with technologies that help organizations provision an employee from the Human Resource (HR) system to other relevant target systems within the enterprise. This is called Enterprise IAM. When Identity and Access Management functions are extended to include customers, partners or other external stakeholders, the traditional Enterprise IAM systems are ill equipped to handle the ever changing and rapidly evolving demands of customers. In these use cases, a specialised Customer Identity and Access Management (CIAM) solution is in order.

This white paper outlines the legal premise of the GDPR, and then delves into the specific parts where Customer Identity and Access Management solutions can help your organization. Please note that these are only our recommendations. In the end, your unique environment dictates how you should approach the GDPR requirements. Thankfully, there are requirements within the regulation that leave wiggle room for interpretation, and will give you some needed flexibility to adopt a solution customised for your organization's needs.

ROLE OF IAM SOLUTIONS IN GDPR

The *raison d'être* of the GDPR is preserving an individual's privacy in a digital world. In the online world, Identity and Access Management (IAM) solutions are the tools that enable your organisation to manage identity related data in a centralized manner. From the GDPR's perspective, managing the scattered and disconnected external identities is much more of a challenge than traditional enterprise identities. Therefore it is natural that Customer IAM plays a more crucial role in achieving GDPR compliance.

While every enterprise environment is different, from the GDPR perspective a one-man company with a single online service and a multi-national enterprise with hundreds of local and global online services have to abide by the same rules. Thus to reach GDPR compliance, CIAM solutions can make the life of a company easier irrespective of its size.

Instead of developing online services with their own user repositories, management functions, registration processes, authentication schemes, authorisation policies etc., IAM can simplify the development of new services by moving all the identity management parts to a centralised solution. The cost of developing this functionality separately for an online service accounts for 30% of the whole budget (of the service development budget). By centralising the IAM functions, organisations can cut costs in service development, streamline existing services, and make it easier to comply with privacy legislation such as the GDPR.

A Customer IAM solution is not the Holy Grail for GDPR compliance. It is a tool to help your organisation comply with the regulation in certain use cases. These use cases become clear when you have done all the preliminary work around the GDPR and you know what kind of data you need to collect, where you collect and manage consent, where you store the data etc. For the sake of brevity, we have highlighted three categories for this whitepaper where CIAM brings clear benefits: Consent management, user data management, and minimum viable data.

CONSENT MANAGEMENT

At the heart of the GDPR is the notion that the end users themselves should be in control of their personal information. Consent is one of the mechanisms put into place to allow online services to continue creating personalized experiences and journeys across channels.

The consent management requirements of the GDPR are perhaps the trickiest to comply with. Online services track users with multiple technologies, including cookies they install to the browser. In order to do that, they must include a cookie policy notice when they see a visitor who hasn't visited the site before, or has deleted their cookies. This is a notice shown after the tracking cookies have already been installed, not asking for consent beforehand.

COLLECTING CONSENT

All of us have come too accustomed to Terms and Conditions over 20 pages long. We ignore them and just click "Agree", and at the same time give tremendous powers to the service we want to use. Under the GDPR, such bulk 'agreements' are specifically deemed null and void in Article 7, Clause 2. When it comes to personal data and GDPR, consent must be given through a clear, positive action for every use case of every user attribute like name or e-mail address. In addition, the user must be able to revoke consent as easily as to grant it. In practise, online services can no longer hide behind legalese about the use of personal data buried in the T&Cs.

Online services can and should be able to collect consent whenever new user attributes are acquired, or they are to be used for a different purpose than before. The first collection point would be during the initial registration, when the end user shares his identity attributes with the service. A second collection point would be when the online service wishes to use or deliver some or all of the identity attributes in a manner that deviates from the original consent.

Example: The user has registered at the Service A and is a frequent visitor. The Service A has formed a new business relationship with a Service B and wishes to offer Single Sign-On from their own service to the Service B. To facilitate the Single Sign-On and ease-of-use for the end users the Service A needs to deliver a set of identity attributes to the Service B when the end user moves from the Service A to the Service B. Before the Single Sign-On can happen, the Service A has to collect consent from the end user and clearly explain what identity attributes are delivered and why.

MANAGING CONSENT

Consent can be seen as a binary state. Either you have the right to use the data as clearly described when collecting the consent, or not. Article 6 of the GDPR underlines the specific cases where you don't

have to collect consent from the user, but in this paper we concentrate on the majority of the use cases - those where collecting consent is required.

It is important that you build a service where your customers can easily review previously given consents and manage them. CIAM solutions with built-in consent management features will allow you to deploy a GDPR compliant consent management system in no time.

PROOF OF CONSENT

A very important part of the GDPR is the reversed burden of proof. If an end user asks for a proof of consent under Article 15, the service must be able to deliver that. There are several ways to do this, the simplest being that you specifically, and securely in order to comply with the processing security requirements set in Article 32, log these events and store them for as long as the consent exists. A CIAM system typically has a very flexible logging subsystem in place, so all events regarding consent can be recorded without spilling personally identifiable information to yet another system.

It is worth noting that merely having consent management where your users can review and manage their consents is not enough to satisfy the requirement for positive proof of consent. For audit and information request purposes you have to be able to show how, when and what was collected, what were the exact terms presented to the user, and any changes or revocations made.

USER DATA MANAGEMENT

PERSONALLY IDENTIFIABLE INFORMATION (A.K.A CUSTOMER INFORMATION)

Once you have decided to collect or have already collected personal information as defined in Article 4, you need to make sure the GDPR requirements are met. The first objective is to discover what type of personal data is stored and prepare the privacy impact assessment. From the cost and security perspective, IAM solutions provide you a centralised repository for storing personal information. In addition, by relinquishing quite a bit of control back to the end user, you can reap the scaling and cost benefits of self-service portals while helping to ensure that the data is up to date.

These are bold claims and deserve a deeper look. Self-service functions and workflows provided by a Customer IAM solution will enable the users to properly view, edit and erase their identity attributes. By allowing greater control for the users, you empower them. When you give the end users a 360° view and ability to manage their own personal data by themselves, it creates trust within the customer base. Trust is a basic building block of business, and therefore the GDPR is not only a regulation to be complied with, it is a business opportunity.

ACCESS TO YOUR OWN INFORMATION

Article 15 of the GDPR states that your customers must have access to their own information. This is something that can be taken for granted these days - at least within the EU. However, if you operate multiple business lines or brands, and during the years you have acquired new services through mergers etc., you might have several isolated identity domains with duplicated user data. Keeping GDPR compliance in mind, you should build a system that allows the end user to access the identity data no matter where it is located within your organisation.

Another aspect of access is naturally authentication. Article 24 of the GDPR requires that “Appropriate technical and organisational measures” are taken to protect the personal information, but does not name those measures like for example mandating multi-factor authentication. Other EU regulations such as eIDAS take a similar approach. However, an absence of any named technology in legislation should not be considered dismissive. It would be a sound business and compliance decision to consider stronger authentication methods and multi-factor authentication. If your organisation is associated with the financial industry, and operates in the EU, the new Payment Services Directive 2 (PSD2) and the regulatory technical standards for strong customer authentication will force you to adopt strong authentication.

MODIFYING YOUR OWN INFORMATION THROUGH SELF-SERVICE WORKFLOWS

Most corporate environments have more than one online service. Without a centralised management solution, it will be very difficult to give a 360° view of the data your organisation possesses about the user. Separated and isolated identity repositories could be easily overlooked.

The role of the CIAM solution is to connect to all existing identity repositories and discover the information stored within, and presenting this information to the user. The end goal is to merge all user information to a single database, and in many cases once a CIAM system has been deployed, the number of separate identity repositories diminishes until there's only the main database left. When the user information is stored centrally and the CIAM system takes care of delivering the required (minimum) set of identity attributes to the applications, your environment takes a big step towards GDPR compliance.

RIGHT FOR ERASURE

Sometimes your customers want to end their relationship with you. When this happens, according to Article 17 of the GDPR the situation is treated as the subject withdrawing consent for all of his attributes. It is clear that having personal data stored in separate and isolated repositories is a dangerous thing. How can you be absolutely certain that all the information has been deleted?

Rather than trying to hunt down user data from dozens of disjoined systems, it makes much more sense to utilise a CIAM solution where a central tenant is to act as a centralised database for user data. This in return turns achieving compliance from battling a multi-headed hydra to a single operation.

RIGHT TO DATA PORTABILITY

Article 20 grants all natural persons an ability to switch service providers and take their personal data with them in a "commonly used and machine-readable format". How this will actually happen regarding data formats etc. is a big question mark, but again having separated and isolated identity repositories will pose a challenge.

MINIMAL VIABLE DATA

NEED TO KNOW

As described in articles 5 to 11, the regulation's central principles are privacy by design and minimal exposure of personal data. Together these can be described as "Need-to-know basis". The term that's

prevalent in Hollywood and James Bond movies aptly describes the practical effect of implementing the various requirements set forth by the regulation. Personal information should only be available to the stakeholders that have a valid and legal reason to process or store the data.

A prime example of unauthorised access to personal information would be a police investigation involving a public figure / celebrity where investigators / officers outside the case access the files. GDPR makes it clear that personal information is off-limits unless you have a valid reason and authorisation to access it. Identity and Access Management can create an environment where access to personal data is controlled and properly logged.

The need to know -principle also extends to data exchange between systems. An application or an online service should only receive the minimum viable data set of the user, both internally and externally. Your own customer-facing application might have unique requirements when it comes to user data. A centrally managed authorisation policy allows you to define which identity attributes are sent to the target system, either without modification or processed/anonymised, e.g. using the birthdate to determine if the user is over 18 years old – and only sending a confirmation to the target system that “The user is at least 18 years old” instead of his or her actual age. When sending data outside of your own organisation, the same policy engine can be used to ensure that you send the minimum set of identity attributes required by the external service.

PRIVILEGED ACCESS MANAGEMENT

Privileged access management is typically associated with administrative users, who can access practically every information system the company has. In this context we refer to people who have unauthorised, legal right to access others’ personal information as privileged users. Where an admin user would use something like Secure Shell (SSH) to access an information system (usually a server), privileged users accessing personal information utilise a client or web application to access the information.

IAM solutions act as gate keepers to personal data. The authentication part will verify the identity of the user, and the authorisation part will determine if the user has the correct permissions to allow access to the data. If the identity is properly verified and the user has the proper authorisation in place, access will be granted. This event will simultaneously be logged for audit or internal review purposes.

IDENTITY ATTRIBUTES

Applications need identity data. Different applications require different sets of attributes. Attributes can be role / authorisation information, name, e-mail, age, address, shoe size, etc. Some of the attributes required by the applications can be derived from the identity data, such as “This user is at least 18 years old”. The CIAM solution will take care a multitude of tasks on behalf of the applications such as

- **Compiling a user profile with just the minimum number of attributes required by the application**
- **Transformation of identity attribute (birthdate → age statement)**
- **Transformation of a technical role to an application role or vice versa**

For your own applications, CIAM provides the tools to keep your architecture simple and focused solely on the core application targets, taking away complex authorisation functions like treatment and transformation of identity data, and finally taking care of authentication at the right level.

When you transfer identity information from your organisation to another organisation either within the EU or outside of the EU, CIAM is the right place to create centralised authorisation policies, where it can be carefully specified what kind of data sets will be sent out. It might be also necessary to collect consent at this point. The user needs to be informed which identity attributes are being sent out, to whom and for what for. Again, CIAM solutions like Ubisecure Identity Server have built-in functionality to achieve this.

CONCLUSION

There are multiple ways how a Customer Identity and Access Management solution can help your path towards GDPR compliance. It is one of the tools data protection officers, CISOs, CIOs, compliance officers, architects and business developers should be aware. But it is not a silver bullet. In this white paper we've outlined a few areas where and how a CIAM solution can be beneficial for your organisation. When all the preliminary tasks towards GDPR compliance are achieved and you start looking for technical solutions to help you start deploying the Privacy by Design principle for your organisation, CIAM can be one of the key technologies.

According to a survey conducted in August 2017 50% of the participants said that achieving GDPR compliance without CIAM would be impossible. The road towards GDPR is 75% about processes and only 25% technology. It is however obvious based on the answers that in some cases the road would have been blocked without CIAM. Link to the survey:

https://www.ubisecure.com/about/resources/ubisecure-ciam-survey-2017/

Ultimately understanding the impact of GDPR to your organisation depends entirely on your environment, processes and data management needs. Contact Ubisecure to discover how we can help.

UBISECURE™

Ubisecure is a pioneering European b2b and b2c Customer Identity & Access Management (CIAM) software provider and cloud identity services enabler dedicated to helping its customers realise the true potential of digital business.

Ubisecure provides a powerful Identity Platform to connect customer digital identities with customer-facing SaaS and enterprise applications in the cloud and on-premise. The platform consists of productised CIAM middleware and API tooling to help connect and enrich strong identity profiles; manage identity usage, authorisation and progressive authentication policies; secure and consolidate identity, privacy and consent data; and streamline identity based workflows and decision delegations. Uniquely, Ubisecure's Identity Platform connects digital services and Identity Providers, such as social networks, mobile networks, banks and Governments, to allow Service Providers to use rich, verified identities to create frictionless login, registration and customer engagement while improving privacy and consent around personal data sharing to meet requirements such as GDPR and PSD2.

Ubisecure is accredited by the Global Legal Entity Identifier Foundation (GLEIF) to issue Legal Entity Identifiers (LEI) under its RapidLEI brand, a cloud-based service that automates the LEI lifecycle to deliver LEIs quickly and easily. The company has offices in London and Finland.

To learn more about Customer IAM and Company Identity solutions visit www.ubisecure.com or contact us at info@ubisecure.com