



## Can we have your ... ? So we can ...

### The CIAM and GDPR journey

- Gustav Gressmann
- 45 years old
- Father of three
- Living in Munich



**Anonymous**

**1**  
Gustav is passionate about cars and is a real petrolhead. He likes to stay tuned with everything cool and upcoming, with a sweet spot for news on exciting sports cars.



**2**  
Gustav dives into the world of car websites and online magazines and decides that 'Awesome Automobiles' brings him the scoops, spyshots, news, reviews and car specification overviews he likes. He subscribes to their daily update first and leaves his email address behind. He however chooses not to create a full profile yet.



**3**  
After a few weeks Gustav is hooked. Based on his active online behaviour he receives an offer for a free one-month trial of the online version of Awesome Automobiles magazine. With this he can access all gated information, including full test reviews, articles, interviews and comparison tests. He can also start personalising his newsfeed and interest on the site and Awesome Automobiles app.



**Pseudonym**

**4**  
To get the trial, Gustav needs to register for an account. He uses the social registration option that is offered, so he can use the same to log in later on. He gives Awesome Automobiles **consent** to use his public Facebook profile. After registration he downloads the app, connects it with his profile and activates push notification.



**6**  
Magazinemonsters wants to reward Gustav for being a loyal customer. He receives an offer for a three-month free trial for a kids' magazine of choice. He receives a unique code to use online.



**Additional info 2**

**5**  
At the end of the trial, Gustav is offered a premium membership, with unlimited access to online content. In addition, he can upgrade at a discount to also receive the weekly printed edition of the magazine. He updates his profile with address, age information and payment information. He **consents** to use his family composition to get special offers from Awesome Automobiles' publisher **Magazinemonsters**, as well as affiliate partners.



**Known**

**8**  
Gustav receives a push notification from his app. He is asked to give **consent** for Happy Horses to use Guinevere's personal data. The purpose, sharing her data with riding schools, is made clear. Gustav gives **consent** by swiping the **consent** button.



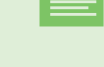
**10**  
After ending the subscription, Magazinemonsters sends a ThankYou email to Gustav and Guinevere, proposing the option of data erasure. Gustav thinks this is a sensible idea and advises her to use this option. Guinevere's data is now removed from the system.



**11**  
Gustav receives a pop-up while logging in to make him aware that Awesome Automobiles is offering a Classic Muscle Car section. He adds preference information and adds his interest to access the Classic Muscle Car content. He also makes a change to his address, because he had made a mistake earlier in the postal code.



**12**  
CarSecure, an affiliate partner of Awesome Automobiles, offers Gustav a 20% discount on his car insurance because of his Awesome Automobiles membership. Gustav is tempted by this offer and decides to change his insurance to CarSecure.



**7**  
Gustav surprises Guinevere, his 12-year old daughter. She chooses an online subscription to 'Happy Horses'. She registers with her Facebook account and the code. She wants to share her data with riding schools in the area to get special offers (like ponycamps, riding lessons, day activities). **Consent** is needed for this purpose. As Guinevere is 12, her parents have to give this **consent**.

**Additional info 3**

**9**  
Guinevere is enjoying her 'Happy Horses' membership, but when the trial period comes to an end, she doesn't want to use her pocket money to continue the subscription.



**Additional info 1**

**13**  
Gustav is routed to the CarSecure site, where he is asked for usage of his profile information held by Awesome Automobiles. After his **consent**, he is requested to check the correctness of this information, change if required and to add missing information in order to complete his CarSecure profile. Upon adding his car registration number, CarSecure performs an online validation with the government's car registration authority and auto-fills all car specifics, required for the insurance. He presses submit and is now a customer of CarSecure.

**Additional info 6**

**14**  
After a year Gustav gets an attractive competing offer from another car insurance, Safe4You. He decides to change his insurance. He uses CarSecure's option to export all his data needed for the contract, to Safe4You.



**15**  
In order to comply with strict anti-fraud regulation, CarSecure operates a data retention policy, that maintains claim history for 7 years. Only required data is stored in encrypted databases and will also be erased automatically after this period.

**Additional info 7**

## Additional Info

**Step 4 & 13:**  
**GDPR article 6:**  
If the processing of data is not covered by one of the bases for processing stated in the GDPR, a consumer needs to give consent to the use of his or her personal data. The use of the data should be linked to one or more specific bases purposes.

**GDPR article 7:**  
Data controllers have to be able to demonstrate that the consumer has consented to processing of his or her personal data. Consumers should also be able to withdraw their consent, just as easy as it was given.

**iWelcome:**  
The Awesome Automobiles website (owned by MagazineMonsters), using the iWelcome CIAM platform, offers social registration and uses consent lifecycle management to ask Gustav for consent to use his Facebook data, while being transparent on the scope of use of all data items. The consents, using the scope of use and the source and the scope of use are stored in the iWelcome CIAM system.

**Step 5:**  
**GDPR article 6:**  
Processing of data can be fair and lawful, for instance, if the data is needed for the performance of a contract. If personal data has only been provided to perform a contract, it cannot be used for any other purpose, unless the data controller asks for specific consent for this new purpose.

**iWelcome:**  
The Awesome Automobiles website, offers a full registration for personal data and payment details. Consent is not needed for these items, because they are necessary for the performance of the contract. In addition, the platform offers the option to enrich a profile with extra information and preferences, in this case family composition. For the use of this additional data, consent should be given.

**Step 7 and 8:**  
**GDPR article 8:**  
Below the age of 16, parental consent must be given when services that require consent are offered directly to a child. European countries have some freedom to implement another age limit, as long as it's not under 13.

**iWelcome:**  
The Awesome Automobiles website is aware that it needs consent from a parent of Guinevere. As Gustav is registered as 'parent' and Guinevere as 'junior member of the family', consent from Gustav will be required.

**Step 10:**  
**GDPR article 17:**  
Every consumer has the right to obtain the erasure of personal data concerning him or her. This applies if the personal data is no longer necessary in relation to the purposes for which it was collected, unless the data (or part of it) has to be kept longer due to regulatory compliance.

**iWelcome:**  
For auditability and to trigger any additional process that may be needed, the system will notify assigned staff (DPO or administrator) of MagazineMonsters that Guinevere made use of her right to erasure. The iWelcome IDaaS platform will remove all Guinevere's data it holds, including any provisioned data in target applications.

**Step 11:**  
**GDPR article 5:**  
Personal data should be adequate, with relevance and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation').

**GDPR article 15:**  
Consumers have the right to know whether or not personal data concerning him or her is being processed and where that is the case, access to the personal data and the purpose of the processing.

**GDPR article 16:**  
Consumers have the right to obtain rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, consumers have the right to have incomplete personal data completed.

**iWelcome:**  
The Awesome Automobiles website and app, offer a 'MyPage' section to manage profile information. On this 'MyPage', Gustav can see all the personal data that MagazineMonsters has stored. He sees what the purpose of processing is (contract, consent, legal, other), can rectify any inaccurate information and can complete any missing information. The system offers a consent-API to store all additional consents from MagazineMonsters and will show Gustav those additional consents in the privacy part of his 'MyPage' with the possibility to withdraw the given consent(s) at any time.

**Step 14:**  
**GDPR article 20:**  
Consumers have the right to receive their personal data in a structured, commonly used and machine-readable format, to transmit the data to another controller. If technically feasible, data can be transmitted directly from one controller to another on request. This is known as the 'right to data portability'.

**iWelcome:**  
CarSecure's website, also using the iWelcome IDaaS platform, has a 'MyPage' that offers the possibility to export personal profile information and to receive that in a machine readable format in an email to the consumer or directly to another data controller (Safe4You). Any further consent lifecycle steps will be handled by the CIAM system of Safe4You.

**Step 15:**  
**GDPR article 5:**  
Personal data should not be kept longer than necessary for the purposes for which the personal data is processed. Apart from processing for commercial reasons, processing for compliance with legal obligations is often necessary, which leads to longer data retention periods.

**GDPR article 6:**  
Personal data can be stored by data controllers in case of legal obligation.  
**GDPR article 15:**  
Consumers have the right to receive information concerning the period for which the personal data will be stored, or if that is not possible concerning the criteria that apply to the duration of the data retention.

**iWelcome:**  
CarSecure, has the possibility to log and store a retention date for every collected data item. This is stored in the metadata of that specific data item. Policy driven data management can constantly verify that metadata and act accordingly. As the metadata is directly connected to the data item in the consumer profile, it can be made visible through the 'MyPage' if desired for transparency purposes.



## Frictionless GDPR

### Delivered by Consumer IAM

**Every EU based company that processes personal data, or non-EU company that interacts with EU citizens, has to be GDPR-compliant from 25th May 2018. Just in case you missed this: GDPR stands for General Data Protection Regulation, and has the purpose to protect the personal data of European citizens.**

Creating an intuitive user experience and maintaining an accurate single view of and towards the consumer, while addressing continuous privacy protection, is the balancing act for today's businesses. It is about building trust by protecting data, by transparent communication throughout the customer journey, by empowering consumers to control their preferences and privacy at any moment and to do this at internet scale. iWelcome's CIAM platform is the enabler for all of this.

#### **iWelcome CIAM – building better relationships for top line growth**

iWelcome improves registration and conversion rates, enhances the personalised user experience (across multiple brands if required). Our platform protects the consumer's privacy and connects them to your organisation and the identity ecosystems you establish. It provides a 360-degree view over the user population in order to support your omnichannel interactions.

This directly fuels top line growth, as strong online relations are the decisive element in future proof or even disruptive business models. It also delivers you the critical element in shielding yourself against uberisation in your industry.

Proof is delivered on a daily basis for tens of millions of consumers in all kinds of industries: health care, media, publishing, (online) retail, insurance, banking and logistic services.

#### **iWelcome CIAM – Privacy Protection embedded in our DNA**

iWelcome is born in the EU and has architected its IDaaS and CIAM platform with EU data protection & privacy in mind. Not just for GDPR, but way before, from day one and from the ground up. Our security and privacy protection capabilities reach far beyond the extensive functionality we provide for our customers to engage with their consumers in line with GDPR. iWelcome can assure data residency in 12 countries, with multi datacenter options in Germany, Switzerland, the UK and US. Our customers have their exclusive private instance, that can be enhanced with high-end additional DDoS and Encryption options. We are not only audited independently for ISO 27001 and SOC 2, but as we are the largest broker in the Dutch eID program also subject to audits from the Dutch Government.

#### **iWelcome CIAM - Consent lifecycle management at the heart**

The GDPR legislation demands a detailed approach to consent lifecycle management. Not only should in certain situations data subjects (the consumers) be asked for consent; as a data controller you have to be able to demonstrate that a consumer has consented to processing of his or her personal data, and for which purpose. Additionally, the consumer should be able to withdraw consent at any time, just as easy as it was given.

In order to build consent management at the heart of digital business driven CIAM, we have seriously changed Identity and Access Management as the industry knew it:

iWelcome introduced the industry's leading CIAM-datamodel, designed to flexibly add attributes and to store preference, interest and profile information. We add metadata to all attributes collected in our platform, to

easily register user consents, internal and external validation. The iWelcome interfaces, consumer facing and for designated staff (like Data Protection Officers) use this metadata to ensure transparency and to enable real time compliance reporting on consent status. As iWelcome is entirely API based, we blend seamlessly with your BI, Marketing and reporting tooling.

#### **GDPR is not a hit and run.**

The challenge is not just to become compliant to GDPR, but to wisely select the right CIAM solution to internalize compliancy in day to day interaction with your consumers.

#### **About iWelcome**

iWelcome provides Identity & Access Management as-a-service (IDaaS). We enable organisations to manage the identity lifecycle and the access rights of their consumers, workforce & business partners in a user friendly and secure manner. As the only European IDaaS provider, we not only assure European data residency, we are also the first platform that is fully GDPR-compliant. Our CIAM platform is rated 'Excellent' by Gartner and named Product and Innovation Leader by KuppingerCole and TechVision.

### Checklist

The 9 most important GDPR requirements your CIAM needs to support

- Consent Management
- Transparency
- Right of Access
- Ability to Withdraw
- Data Portability
- Right to Erasure & Rectification
- Privacy by Default & Design
- Data Retention
- Security by Design