GDPR and CAR

GDPR is an EU initiative that will have significant consequences not just on practices within European countries but on organizations world-wide that provide services to EU citizens. It lays out a number of requirements on the proper use, and non-use, of consent in attribute and personal information release.

It is too early for there to be a "reference implementation" of GDPR compliance when consent is used. Below is a partial list of GDPR requirements, and an assessment of how CAR addresses those requirements.

Consent must be opt-in with affirmative actions in the UI. It must be freely given.

CAR is designed for opt-in support, and, via the admin policy settings, be limited in use to those use cases where consent is freely-given. Dialogue boxes shift as appropriate to reinforce affirmative actions.

Consent should be "specific".

CAR can provide consent on a per site basis and a per application basis.

Consent should be just in time, given as close as possible to the time an app needs the attributes.

The architecture of federated identity provides for just in time release as a primary mode of use. CAR also permits a "while I'm away" consent mechanism and suppressing that consent dialogue after initial consent is given.

Consent should not be a part of a general ToS click through; it must be explicit and unambiguous.

Using CAR, consent is a distinct activity, as a technology and as a user experience from accepting the ToS of a specific service or application.

Consent should allow for purpose limitation on the attributes being released.

CAR does not address this directly. Such limitations can be part of a larger legal or trust infrastructure that CAR taps into.

Consent must be clear and simple. It should be concise and well-tailored.

The CAR UI has gone through extensive user testing. Managing the cognitive load for the user has been a prime design consideration.

Consent must be revocable.

Through the self-service UI, CAR provides users with ready capability to change their current attribute release policy for any of their site, which revokes existing settings.

Fine grain release, data minimization and required vs optional

This set of related concepts are central to GDPR and to CAR. CAR is designed to do fine grain release, and has several mechanisms to control how required attributes are presented to the user.

Consent must be informed.

CAR has several mechanisms to inform users. In the user management UI there are settings to indicate what the IdP recommends and, eventually, why. In addition, trust marks are being added to the end-user UI so that the user can find more information about the relying party.

GDPR calls for special UI handling for sensitive values.

CAR has important concepts such as sensitive attributes (every value is sensitive) and sensitive values (the attribute is not inherently sensitive but certain values are). A superadmin can set the handling of these (such as do not display on screen unless explicitly requested by the user.)

Consent should provide an audit trail with cryptographic protection.

CAR keeps an audit trail that is cryptographically protected. The audit trail contains the hash of sensitive information to protect privacy. There will also be the capability to issue notifications via sec events and other mechanisms.

“GDPR makes consent very strict. Organizations might view this as an additional burden. But in reality it will allow to establish **consent as one of the trust factors connecting users and organizations offering services**.”

- Lukasz Olejnik