EU General Data Protection Regulation (GDPR)

Regulation Excerpts: Identifying Users

v3.0

Copyright ©2017 aPersona, Inc.

GDPR Compliance Req'd by May 25, 2018

Multi-Factor Authentication: GDPR Compliance Req'd by May 25, 2018

- Organizations with any PII data in the EU, are to have policies that use all reasonable identifiers to verify the identity of users requesting access to on-line services as a "default protection". It is permissible to use identifiers to create a "User Profile" to identify users.
  Organizations providing services to people in the EU "should" be required to follow GDPR guidance and be subject to the regulation as well.

- There are two types of Identifiers defined in GDPR:
  - "Unique Personal Identifiers" (ID's, Passwords, PINs, Account Numbers, etc.) and
  - "Online Identifiers" (devices, tools, protocols, IP Addresses, Cookie Identifiers, RF Tags, etc.)

https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Copyright ©2017 aPersona, Inc.

GDPR Excerpts

GDPR:

1. "identifiable natural person" = "data-subject" = "identifiable natural person" = "unique person"
2. Person's are considered "uniquely identifiable" if they have an "identifier" assigned to them such as an ID number or online identifier.
3. Natural persons may have online identifiers provided by their devices, applications, tools protocols such as IP Addresses or cookie IDs.
4. Controllers should use all reasonable measures to verify the identity of a data subject requesting access.
5. It is permissible to use online identifiers and unique identifiers to create a "User Profile" in order to identify users.

Article 4

Definitions

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

L 119/6 EN Official Journal of the European Union 4.5.2016

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

L 119/12 EN Official Journal of the European Union 4.5.2016

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Online Identifiers Defined:

- Devices
- Applications
- Tools & protocols
- Internet IP Addresses
- Radio frequency ID Tags

Unique Identifiers

It's permissible to use identifiers to create a "Profile" of identifiers to identify people.

Copyright ©2017 aPersona, Inc.

GDPR Excerpts

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

Risk evaluations include the risks presented by unlawful access to personal data.

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

Risk must be evaluated and used to ensure security measures match the risks.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Risk evaluations must include the risks presented by unauthorized access to personal data.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. …

Default security POLICIES should be "ON" for all users by default. (Not an Opt-In implementation.)

Copyright ©2017 aPersona, Inc.

GDPR Excerpts

(39) Any processing of personal data should be lawful and fair... Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

Companies providing services to people who reside in the EU "should" be subject to GDPR. It would be advisable for these companies to not ignore GDPR Guidance.

Copyright ©2017 aPersona, Inc.

aPersona & GDPR

aPersona capabilities that address GDPR

- aPersona invisibly creates profiles of unique identifiers and on-line identifiers.
- These profiles are evaluated against specific Policies based on risk.
- Policies provide security by “default” and are used to identify users for logins and transactions.
- Policies are completely adaptive and provide the necessary risk evaluations using all available identifiers and is essentially invisible to end users at the same time.

Contact us at: info@apersona.com

Copyright ©2017 aPersona, Inc.