Infomedia Limited

Statement on GDPR compliance

Table of Contents

Version Control

Version #	Approved By	Revision Date	Reason
V1.0	Mark Grodzicky – Data Protection Officer	20/3/2018	For Customer and supplier distribution. Also available at www.infomedia.com.au/gdpr

Document References

This document should be read in conjunction with the following documents:

Name	External Public Access Location
Data Processing Agreements with Infomedia's main Third-Party Processors	www.infomedia.com.au/gdpr
Proforma Data Processing Agreement used by Infomedia	www.infomedia.com.au/gdpr
Infomedia Privacy Policy	www.infomedia.com.au/privacy
Infomedia End User Licence Agreements (EULA)	www.infomedia.com.au/eula

1 Introduction

Infomedia is committed to comply with privacy and data privacy protection laws in all jurisdictions where it does business.

Ensuring data privacy protection is the foundation of trust and maintaining the reputation of the Infomedia Group in all its commercial relationships.

This Guide has been prepared to provide customers and suppliers details of how Infomedia complies with the data protection laws prescribed by the European Union Data Protection Directive (GDPR) and the European Economic Area (EEA). It also applies to our compliance program with other privacy and data protection laws such as Australian Privacy Act, the UK Data Protection Act and the US Privacy Shield.

2 Document Purpose

The purpose of this document is to set out Infomedia's guide to how Infomedia complies with the EU GDPR requirements that impact Infomedia's operations and applications used by our customers, which becomes effective on 25th May 2018.

It is supported by Infomedia's privacy policy which can be found at www.infomedia.com.au/privacy.

3 Summary of GDPR

The European Union's Data Protection Directive 95/46/EC, adopted in 1995, regulates the protection of individuals with regards to the processing of personal data and the free movement of such data.

The European Union Commission has issued updated privacy laws commonly referred to as General Data Protection Regulations (or GDPR) and which will take effect on 25th May 2018.

Further information on GDPR can be found on the EU GDPR Portal at http://www.eugdpr.org/

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world.

Below are some common definitions used by the GDPR and in this document:

"Personal Identifiable Information" (PII) 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.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose means of the processing of PII. In most cases the party initially collecting the PII is the Data Controller. They are the party that needs to "control" the use and security of PII, need to obtain consent for its collection and use and is primarily liable for data breaches.

"Data Processor" means the natural or legal person, public authority, agency or other body which processes PII on behalf of the Data Controller. Processing means any operation or set of operations which is performed on PII or on sets of PII, whether or not by automated means.

With some exceptions, processing of PII is only lawful if the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes.

The Data Subject has the right to request the Data Controller to erase PII concerning him or her without undue delay (right to be forgotten).

The GDPR apply to all companies processing PII of Data Subjects residing in the European Union, regardless of the company's location. The GDPR also applies to the processing of PII of Data Subjects in the EU by a Data Controller or Data Processor not established in the EU (eg. such as in the USA or Australia), where the activities relate to offering goods or services to EU citizens.

We have assessed that the GDPR applies to Infomedia as a Data Processor of PII on behalf of our customers (such a dealers and OEM's) who use our applications as part of their business and as a Data Controller for customer PII we collect ourselves and store and process in our sales, marketing and internal operational systems.

4 Summary of US Privacy Shield

The United States has, as part of negotiations and agreement with the EU, established a Privacy Shield framework to allow US based companies who sign up with the Privacy Shield to comply with the GDPR and transfer Personal Identifiable Information (or PII) from the EU to the USA.

This replaced the former Safe Harbour framework which the EU Commission held in 2015 was inadequate.

See https://www.privacyshield.gov

On July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law.

On January 12, 2017, the Swiss Government announced the approval of the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States.

It is a voluntary scheme that US companies can apply for to certify that they will comply with privacy laws and be subject to enforcement, including under the GDPR.

Infomedia is certified under the US Privacy Shield.

5 Infomedia Privacy Policy

The Infomedia Privacy Policy explains how and why Infomedia collects personal information, how it is used, and what controls a Data Subject has over Infomedia's use of it.

Infomedia is committed to complying with applicable laws governing the collection and use of personal information and to protecting and safeguarding a Data Subject's privacy when that person deals with us.

The Infomedia privacy policy can be found on at www.infomedia.com.au/privacy

6 Data Security and Protection

Infomedia has adopted the ISO27001 framework standard as the basis for its data security procedures and processes.

Infomedia, as a Data Processor, when processing PII on behalf of a Data Controller in connection with services provided by Infomedia, has implemented and maintains the following technical and organizational security measures for the processing of such PII:

1. **Physical Access Controls**: Infomedia has implemented reasonable measures to prevent physical access, such as secured buildings and access controls within premises, to prevent unauthorized persons from gaining access to PII, and ensure Third Parties such as those operating data centres are also adhering to such controls.
2. **System Access Controls:** Infomedia has implemented reasonable measures to prevent PII from being used without authorization. These controls vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.
3. **Data Access Controls:** Infomedia has implemented reasonable measures to ensure that PII is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the PII to which they have privilege of access; and, that PII cannot be read, copied, modified or removed without authorization in the course of Processing.
4. **Transmission Controls:** Infomedia has implemented reasonable measures to ensure that it is possible to check and establish to which entities the transfer of PII is made by means of data transmission facilities so PII cannot be read, copied, modified or removed without authorization during electronic transmission or transport.
5. **Input Controls:** Infomedia has implemented reasonable measures to allow it to check and establish whether and by whom PII has been entered into data processing systems, modified or removed and to ensure that (i) PII is under the control of Data Controller; and (ii) PII is managed by secured transmission from Data Controller.
6. **Data Backup and retention:** Infomedia has implemented measures to ensure that back-ups of relevant databases are taken on a regular basis, are secured to ensure that PII is protected against accidental destruction or loss. PII will be securely deleted or erased when it is no longer needed for a permitted business purpose.
7. **Logical Separation:** Infomedia has implemented measures to ensure that PII from different Infomedia subscriber environments is logically segregated on its systems to ensure that PII that is collected for different purposes is processed separately.

7 Infomedia Compliance with GDPR

Infomedia has set in place a program and policies to ensure that it will comply with the GDPR, which comes into effect on 25th May 2018.

The details are set out in the table below to help demonstrates how Infomedia complies with GDPR:

GDPR	Infomedia Compliance
Consent	*Infomedia as the data controller*: Infomedia obtains consent to capture and process PII as part of the initial collection process and only processes PII for the purposes covered by the consent and according to our privacy policy. *Infomedia as the data processor:* It is the responsibility of the Data Controller (eg. dealer or OEM who collects the customer PII) to obtain consent. The Data Controller needs to ensure that they have consent for any PII they collect, enter or transfer into Infomedia's applications (as Data Processor). This obligation is included in Infomedia's contracts. Infomedia processes and stores PII according to GDPR requirements as a data processor.
Data security and protection	Infomedia has adopted the ISO27001 standard as the basis for its data security procedures and processes. ISO27001 is an information security standard that is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee. It is an internationally recognised standard for the specification of an information security management system (ISMS). This ensures that security and protection is part of our systems by design and by default.
Location of PII data storage for customer applications	Infomedia stores PII processed by our applications using Amazon Web Services (AWS) infrastructure. Subject to the terms of our customer agreements, PII captured and processed by our EU customers will be stored in zones in the EEA, in an adequate jurisdiction (as defined by the EU under the GDPR) including in the USA as envisaged under the US Privacy Shield and / or Data Processing Agreement.
Data Processing Agreements	Infomedia has available as a proforma Data Processing Agreement (DPA) to our customers to sign. The DPA allows the data subject of the PII to obtain recourse from the data processor should there be a breach of PII data security. The DPA is based on and adopts the 'Model Clauses' approved by the EU. While we expect our customers will want to sign the DPA, the lack of a signed DPA will not prevent us from continuing to provide services to

	our customers. A template of the DPA is available at http://www.infomedia.com.au/gdpr/
Data Protection Officer	The GDPR requires Infomedia to appoint a Data Protection Officer (DPO) to be involved properly and in a timely manner in all issues which relate to the protection of personal data. Infomedia has appointed Mark Grodzicky, our General Counsel, to this position. He reports directly to our CEO and can be contacted by email at privacy@infomedia.com.au
3rd party suppliers	Infomedia uses 3rd party suppliers as Data Processors to provide us with hosting, processing, applications and other services used to provide the Infomedia application and process PII, including AWS, Zendesk, Microsoft, Auth0 and Netsuite (now part of Oracle). Infomedia has signed DPAs with these data processors and is satisfied that these suppliers provide adequate protection under GDPR for PII. Copies of those agreement are available at http://www.infomedia.com.au/gdpr/
Amazon Web Services (AWS)	Amazon Web Service (AWS) is a key 3rd party data processor as Infomedia's cloud infrastructure service provider. Infomedia has signed a DPA with AWS, as available at http://www.infomedia.com.au/gdpr AWS is responsible for the security of the cloud infrastructure used by Infomedia. AWS provides highly secure data centres utilizing state-of-the art electronic surveillance and multi-factor access control systems. Data centres are staffed 24x7 by trained security guards and access is authorized strictly on a least privileged basis, limited to system administration purposes.
Special categories of personal data	The GDPR mandates greater security and controls when processing of certain special categories of PII, such as financial and health data. Infomedia does not currently and does not plan to process or capture special category PII. Infomedia does not collect or store credit card details but may use third party payment gateways such as PayPal to allow customer to make any credit card payments.
Support systems, email, chat and instant messages	Information sent to Infomedia or entered into Infomedia support systems and applications may be transferred outside of the EEA. The Data Controller sending PII data or entering PII data into these Infomedia systems is responsible for ensuring that they have the necessary consent of the Data Subject to provide the PII and if required, enter into a DPA with Infomedia.
Right to access	Due to its nature, Infomedia has assessed the likelihood of requests to access the PII stored as a Data Controller as low. The same assessment applies to PII stored by Infomedia as a Data Processor in our applications by our customers.

	Should we receive a request to access PII, we can provide, subject to verification of the Data Subject, such PII on a case by case basis.
Data portability	Due to its nature, Infomedia has assessed the likelihood of requests to port PII we store as Data Controller as low. The same assessment applies to PII stored by Infomedia as a Data Processor in our applications by our customers. Should we receive a request to provide PII, we can provide, subject to verification of the Data Subject, such PII data in an agreed format on a case by case basis.
Right to be forgotten	Due to its nature, Infomedia has assessed the likelihood of requests to erase PII we store as a Data Controller as low. The same assessment applies to PII stored by Infomedia as a Data Processor in our applications by our customers. Should we receive a request for PII to be erased, we can, subject to the verification of the Data Subject, erase such PII on a case by case basis.
Breach notification	Infomedia will comply with the breach notification requirements in Article 33 of the GDPR which provides that a personal data breach must be reported unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
Staff and contractor training	Infomedia has implemented a mandatory on-line training program to ensure all staff and contractors are trained in privacy and information security.