



Infomedia Limited and subsidiaries

Statement on privacy compliance
including European Union
General Data Protection Regulation
(GDPR)

Table of Contents

Versions.....	2
Document References.....	2
1 Introduction.....	3
2 Document Purpose	3
3 Summary of GDPR.....	3
4 US Privacy Shield (now held to be inadequate).....	4
5 Infomedia Privacy Policy – as a Data collector / Controller	4
6 Infomedia as a Data Processor	4
7 Data Security and Protection.....	5
8 Infomedia Compliance with Privacy Laws, including GDPR.....	6
9 Third party Processors and GDPR	9

Versions

Version #	Approved By	Revision Date	Reason
V1.0	Mark Grodzicky – DPO	20/3/2018	For Customer and supplier distribution. Also available at www.infomedia.com.au/gdpr
V2.9	Mark Grodzicky – DPO	19/6/2018	Updates
V 3	Mark Grodzicky – DPO	9/8/2018	Added ISO 27001 certification
V 4	Mark Grodzicky – DPO	19/10/2020	Update re US Privacy Shield and general updates
V 5	Mark Grodzicky – DPO	15/12/2021	Additional sections, Updates in general

Document References

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

Document Name	External Public Access Location
Data Processing Agreements with Infomedia’s Main Third-Party Processors	www.infomedia.com.au/gdpr
Intercompany Data Protection Agreement between Infomedia Group Companies	www.infomedia.com.au/gdpr
Proforma Data Processing Agreement based on Standard Contractual Clauses (June 2021)	https://www.infomedia.com.au/privacy-compliance/#tab-1629354553993-8
Infomedia Privacy Policy	www.infomedia.com.au/privacy
Infomedia End User Licence Agreements (EULA)	www.infomedia.com.au/eula
ISO 27001 Statement of Certification issued by Best Practice	https://www.infomedia.com.au/certificates/

1 Introduction

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

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 privacy laws globally, including the data protection laws prescribed by the European Union Data Protection Regulation Directive (GDPR) and the European Economic Area (EEA) and other privacy and data protection laws such as the Australian Privacy Act, United States privacy laws including the California Consumer Privacy Act and the UK Data Protection Act.

2 Document Purpose

The purpose of this document is to set out Infomedia's guide how we comply with privacy laws worldwide that impact Infomedia's operations and applications used by our customers.

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) which took 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 guide):

"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. In most cases, this will be the car dealership or the OEM.

"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. Infomedia is generally a Data Processor.

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 applies 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 European Union 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 as automotive 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 US Privacy Shield (now held to be inadequate)

The United States, as part of negotiations and agreement with the European Union in 2015, established a Privacy Shield framework to allow US based companies who sign up to comply with the GDPR and transfer Personal Identifiable Information (or PII) from the EU to the USA. See <https://www.privacyshield.gov>

This replaced the Safe Harbour framework which the EU Commission held in 2015 was held to be inadequate the Court of Justice of the European Union.

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.

On July 16, 2020, the Court of Justice of the European Union issued a judgment declaring as "invalid" the European Commission's Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield. As a result of that decision, the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. This decision does not relieve participants in the EU-U.S. Privacy Shield of their obligations under the EU-U.S. Privacy Shield Framework.

The U.S. Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List.

Infomedia was certified under the US Privacy Shield but withdrew in October 2020. Infomedia will rely on the intercompany data protection agreement to transfer data between its subsidiaries.

5 Infomedia Privacy Policy – as a Data collector / Controller

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. This include marketing, administration, user logins and related activities.

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 Infomedia as a Data Processor

Where dealership or OEM customers use our products to provide services to their car owners (and who may provide personal identifiable information as part of those services), Infomedia is a Data Processor only.

The dealership or the relevant OEM is the Data Collector / Controller and instructs Infomedia as to how it should process that customer data, how long it should be retained, what consents it has obtained to use that data, all as generally set out in the dealership or OEM privacy policy.

Infomedia does not share or otherwise use that customer personal identifiable information except as instructed by the Data Collector/Controller.

7 Data Security and Protection

Infomedia has adopted the ISO27001 framework standard as the basis for its data security procedures and processes and is certified by Best Practice Certification Pty. Ltd Certificate Number 63003326431 expiry 06/08/2024

Infomedia, both as a Data Controller and also when acting as a Data Processor (eg 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.

8 Infomedia Compliance with Privacy Laws, including GDPR

Infomedia has set in place a program and policies to ensure that it will comply with the privacy laws worldwide, including the GDPR.

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

Privacy Law Requirement	Infomedia Compliance
Consent	<p><i>Infomedia as the data controller:</i></p> <p>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 the Infomedia privacy policy.</p> <p><i>Infomedia as the data processor:</i></p> <p>It is the responsibility of the Data Controller (eg. dealer or OEM who collects their customer PII) to obtain consent in line with their own privacy policy. 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 instructions of the Data Controller as a data processor.</p>
Data security and protection	<p>Infomedia has adopted the ISO27001 standard as the basis for its data security procedures and processes.</p> <p>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).</p> <p>Adoption of this standard ensures that security and protection is part of our systems by design and by default.</p>
Location of PII data storage for customer applications	<p>Infomedia stores PII processed by our applications using Amazon Web Services (AWS) infrastructure as follows:</p> <ul style="list-style-type: none"> a) From EU customers will be stored in the EEA, in an adequate jurisdiction (as defined by the EU under the GDPR) including in the USA as envisaged under the Intercompany Data Processing Agreement. b) For US and Canada customers, in the USA c) Elsewhere in the world, in either of the above locations or in Australia
Dealership / OEM Customer PII	<p>Infomedia does not access or share any Dealership / OEM customer PII, except for resolving any reported errors in the applications.</p> <p>The Dealership / OEM is responsible for the collection and use of such customer PII, including its update and deletion.</p>
Data Processing Agreement (DPA)	<p>A DPA allows the data subject of the PII to obtain recourse from the data processor should there be a breach of PII data security.</p> <p>Infomedia has developed a proforma Data Processing Agreement (DPA) for our customers to sign as required by the GDPR. The DPA is based on</p>

	<p>and adopts the ‘Model Clauses / Standard Contractual Conditions’ as approved by the European Union in June 2021.</p> <p>A template of the DPA is available at http://www.infomedia.com.au/gdpr/</p>
Data Protection Officer	<p>Privacy Laws in general require Infomedia to appoint a Data Protection Officer (DPO) or similar to be involved properly and in a timely manner in all issues related to the protection of personal data.</p> <p>Infomedia has appointed Mark Grodzicky, our General Counsel, to this position. He reports to our CFO and can be contacted by email at privacy@infomedia.com.au</p>
Special categories of personal data	<p>Privacy laws in general mandate greater security and controls when processing of certain special categories of PII, such as financial and health data.</p> <p>Infomedia does not currently and does not plan to collect or process special category PII.</p> <p>Infomedia does collect credit card details in a limited number of circumstances and may use third party payment gateways such as PayPal to allow customer to make credit card payments.</p>
Support systems, email, chat and instant messages	<p>Information sent to Infomedia or entered into Infomedia support systems and applications may be transferred outside of the origin country, as we use Microsoft 365 Office and other cloud based solutions.</p> <p>Data Controllers wanting to send PII data or entering PII data into these Infomedia support systems is responsible for ensuring that they have the necessary consent of the Data Subject to provide the PII, that it is secure in transmission and if required, enters into a DPA with Infomedia.</p>
Right to access	<p><i>Infomedia as the data controller:</i></p> <p>Data Subjects who have provided their PII to Infomedia as a Data Controller (eg if we have included them on our marketing lists) may request to access that data by sending an email to privacy@infomedia.com.au and may need to provide verification data.</p> <p><i>Infomedia as the data processor:</i></p> <p>Each Data Controller (eg Dealership or OEM) can access and modify, including update and deletion, of PII that it has entered into the relevant Infomedia applications via the application interface.</p> <p>Should we receive a request as Data Processor to identify right to access PII, we will refer that request to the relevant Data Controller. If the Data Controller is unable to delete or modify the PII, Infomedia can provide a quote, to delete or modify such PII on a case by case basis. The Data Controller is responsible for verification of the Data Subject.</p>
Data portability	<p><i>Infomedia as the data controller:</i></p> <p>Data Subjects who have provided their PII to Infomedia as a Data Controller (eg if we have included them on our marketing lists) may request to port that data by sending an email to privacy@infomedia.com.au and may need to provide verification data.</p> <p><i>Infomedia as the data processor:</i></p>

	<p>Each Data Controller can access and modify, including export, of PII that it has entered into the relevant Infomedia applications via the application interface.</p> <p>Should we receive a request to as Data Processor to port PII, we will refer that to the relevant Data Controller. If the Data Controller is unable to port the PII, Infomedia can provide a quote, to port the PII on a case by case basis. The Data Controller is responsible for verification of the Data Subject.</p>
<p>Right to be forgotten</p>	<p><i>Infomedia as the data controller:</i></p> <p>Data subjects who have provided their PII to Infomedia as a Data Controller (eg if we have included them on our marketing lists) may request to delete that data by sending an email to privacy@infomedia.com.au and may need to provide verification data.</p> <p><i>Infomedia as the data processor:</i></p> <p>Each Data Controller can access and modify, including deletion, of PII that it has entered into the relevant Infomedia applications via the application interface.</p> <p>Should we receive a request as the Data Processor for PII to be erased, we will refer that to the relevant Data Controller. If the Data Controller is unable to erase the PII, Infomedia can provide a quote, to erase the PII on a case by case basis. The Data Controller is responsible for verification of the Data Subject.</p>
<p>Breach notification</p>	<p>Infomedia will comply with the privacy law breach notifications, including the requirements in Article 33 of the GDPR.</p> <p>In general these require 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 or cause serious harm.</p>
<p>Staff and contractor training</p>	<p>Infomedia has implemented a mandatory on-line training program to ensure all staff and contractors are trained in privacy and information security.</p>
<p>Retention of data</p>	<p><i>Infomedia as the data controller:</i></p> <p>Infomedia will review and delete PII provided by Data Subjects who have provided their PII to Infomedia as a Data Controller (eg if we have included them on our marketing lists) when there is no longer a business need to retain that, or when requested to delete by the data Subject.</p> <p><i>Infomedia as the data processor:</i></p> <p>As applications provided by Infomedia are tools to be used by Data Controllers, Infomedia does not manage or set any time period limits to retention of PII, as this remains the responsibility of the Data Controller.</p> <p>Each Data Controller can access and modify, including deletion, of PII that it has entered into the relevant Infomedia applications via the application interface.</p>

9 Third party Processors and GDPR

<p>3rd party suppliers</p>	<p>Infomedia uses 3rd party suppliers as Data Processors to provide us with hosting, processing, applications and other services used to provide the Infomedia applications and process PII, including AWS, Auth0, DocuSign, Microsoft, MongoDB, Netsuite (part of Oracle), New Relic and Zendesk.</p> <p>Infomedia has signed data processing agreement (DPAs) with these data processors and is satisfied that these suppliers provide adequate protection under GDPR for PII. Note that many of these processors also use subprocessors, most of which are the same companies (eg AWS provides a range of services to many processors).</p> <p>We review these and ensure that those subprocessors are also suitable and will provide adequate protections. Some of these also do not have access any PII and simply provide application performance and other related services.</p> <p>Copies of 3rd party Processor DPA's are available at https://www.infomedia.com.au/gdpr</p>
---------------------------------------	---