BeSoftware - GDPR Assessment and Evaluation Report

Version : 1.0
16 May 2018

Document Control

Document Information

Name	BeSoftware - GDPR Assessment and Evaluation Report_v1.0MQ.docx	Version	1.0	Updated	16 May 2018

Document Contributors

Name	Role	Phone	Email
Martin Quinn	Author	(02)8060 1113	marting@intactsecurity.com.au
Elin Ousback	Quality Assurance	(02)8060 1113	elino@intactsecurity.com.au

Client Sponsor

Name	Role	Phone	Email
Renato Parletta	CEO		renato.parletta@besoftware.biz

1.0 Executive Summary

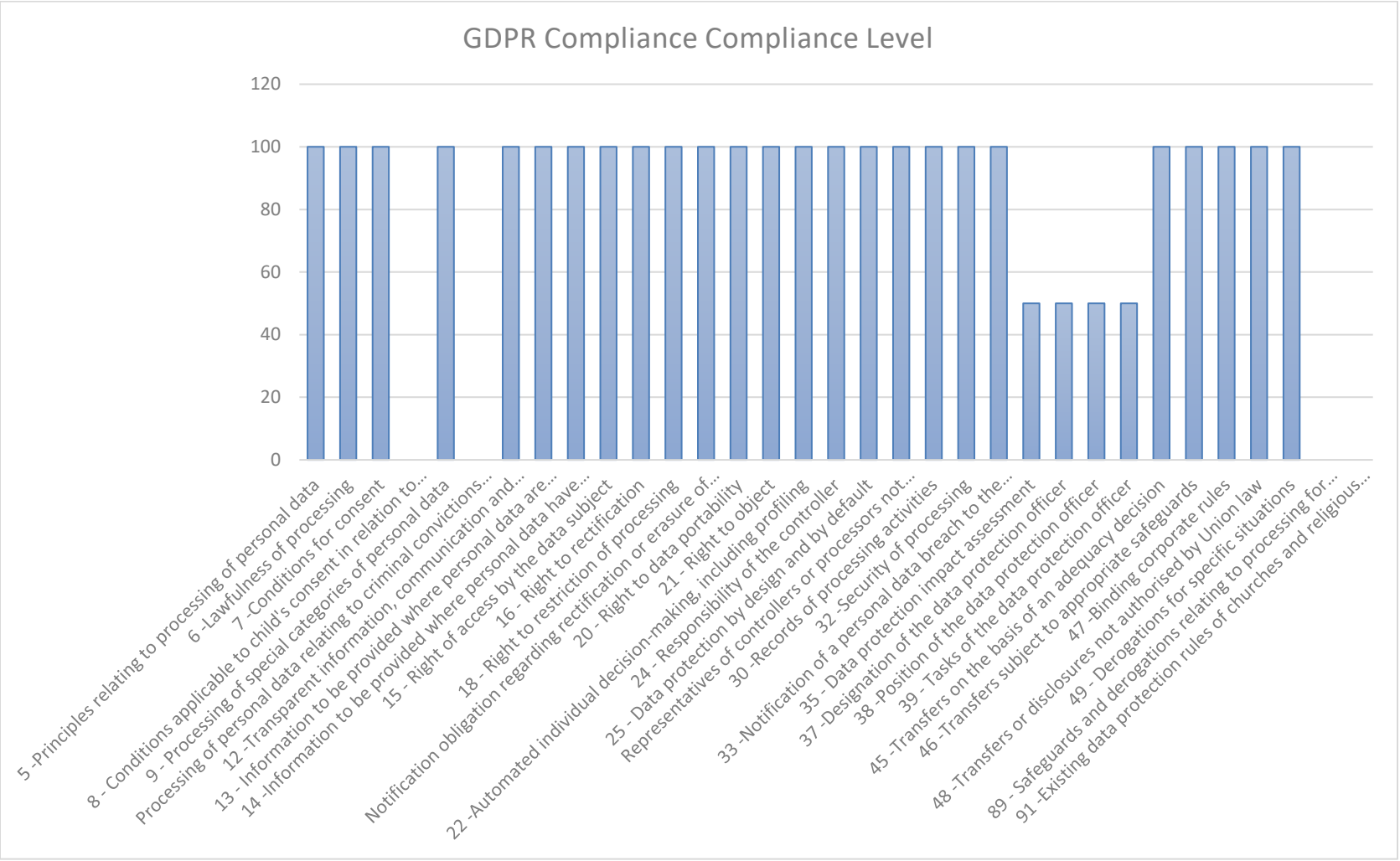
Intact Security was engaged by BeSoftware to perform an assessment/attestation of the BeSoftware as it relates to the European Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)). Intact Security conducted an compliance assessment of the BeSoftware system and documentation as it relates to GDPR to ascertain whether BeSoftware was performing duties in accordance with the GDPR articles 1- 99. The GDPR is developed with the principle of providing data protection regarding personally identifiable data for European citizens, with a baseline of generic risks and controls associated with the storage and handling of sensitive information. This is designed to ensure consistency and appropriate control across organisations who are either defined as Data Controllers or Data Processors.
GDPR requires that the data control, use and storage is based on sound security principles and to determine whether the security measures chosen by the Data Controller/Processor have been implemented and are operating effectively.
The GDPR Assessment of the BeSoftware systems was undertaken in May 2018.
A high degree of compliance with the GDPR was evident, as BeSoftware had already fostered a culture of compliance and control regarding data in alignment with ISO/IEC 27001:2013 and the Australian Signals Directorate IRAP program.

The Assessor confirmed that the BeSoftware systems architecture was based on sound security principles and that all of the requirements of the GDPR had been considered as part of the solutions design when considering BeSoftware as a Data Controller. The implementation of the foundational components of the BeSoftware system does provide and appropriate level of information security mechanisms in support of protecting data. A minimal level of non-compliance was observed, however BeSoftware was in the process of addressing these shortfalls with the expectation that over time this will improve and be compliant.

The Intact Security assessment methodology required the assessor to inspect each individual GDPR article/control, instead of random control sampling. This methodology was used so that the level of assurance demonstrated BeSoftware's adoption of the GDPR requirements.

Where the Assessor was unable to validate an a control as implemented and operating effectively, a finding of Not yet Implemented was made. Where possible, the Assessor confirmed that each applicable control was technically implemented in the BeSoftware system and where feasible the Assessor performed additional testing which validated each controls effectiveness. This approach ensured that the Assessment was comprehensive and that the assessment report accurately documented the BeSoftware systems security risk and compliance posture as it relates to GDPR.
The assessor, assesses the overall level of GDPR compliance associated with the BeSoftware systems to be **HIGH** and be operating affectively.
With regards to the integrity of private/personally identifiable information/data, the assessor understands that appropriate backups are in place for the underlying solution as the Data Controller. The loss of data is not expected to occur based on the resilience of the architecture provided by both the Data Controller and Data Processor.
The assessor ensured that all controls assessed as non-compliant have been promptly communicated to BeSoftware during the course of the assessment. BeSoftware are currently considering alternative or compensating controls in order to mitigate the risks associated with the identified instances of non-compliance.

1.1 Compliance by GDPR Chapter



2.0 Assessors Statement

I advise that the BeSoftware systems are compliant with the applicable GDPR articles and controls.

The associated non-compliance has been identified and assessed an overall **LOW to MEDIUM** risk. The level of risk is due to the inability of the assessor to validate that all applicable controls were operating effectively at the time of the assessment. LOW to MEDIUM risk is able to be accepted by BeSoftware and can be managed through standard operational security practices which includes effective contract management.

The assessor recommends that BeSoftware continue to improve and elevate the security posture of the BeSoftware systems, give focus to the development of the DPIA and formally document the roles and responsibilities of the DPO to become fully compliant.

Martin Quinn
ISO27001 Lead Auditor and IRAP Assessor

3.0 Related Law/Regulations/Policies

The following Australian legislation is relevant to this Report:

- Archives Act 1983
- Copyright Act 1968
- Crimes Act 1914
- Criminal Code Act 1995
- Cybercrime Act 2001
- Electronic Transactions Act 1999
- Evidence Act 1995
- Financial Management and Accountability Act 1997
- Freedom of Information Act 1982
- Privacy Act 1988
- Public Service Act 1999
- Spam Act 2003
- Surveillance Devices Act 2004
- Telecommunications (Interception) Act 1979

The following European Legislation is relevant to this Report:

- European Regulation (EU) 2016/679 (General Data Protection Regulation