REGULATION (EU) 2016/679
General Data Protection Regulation

An overview to the new legal data protection requirements impacting on all businesses trading within the EU

John Greenwood – Compliance3
June 2016

Compliance3
Compliant Contact Centres. *Delivered.*

GDPR: a new citizens charter for Europe

GDPR background: what, why and when?

- The EU GDPR is a European wide regulation focussing on the protection of all personal information by any organisation operating within Europe – An EU Citizens charter

- There was previously no EU wide standard, each individual country had their own standard, many of which had not been updated since the early 1990's

- 4 years in the making and became effective on 24th May 2016 and must become law in each Member State by 25th May 2018

- Applies to all global entities trading with EU citizens in Europe

Regulation (EU) 2016/679: GDPR the document and positioning

- 173 ‘whereas’ positioning statements covering 31 pages
- 11 Chapters and 99 Articles across 57 pages
  - Chapter I – General Provisions (Articles 1 to 4)
  - Chapter II – Principles (Articles 5 to 11)
  - Chapter III – Rights of Data Subject 5 Sections (Articles 12 to 23)
  - Chapter IV – Controller & Processor 5 Sections (Articles 24 to 43)
  - Chapter V – Transfers of Personal Data (Articles 44 to 50)
  - Chapter VI – Independent Supervisory Authorities (Articles 51 to 59)
  - Chapter VII – Cooperation & Consistency (Articles 60 to 76)
  - Chapter VIII – Remedies, Liability & Penalties (Articles 77 to 84)
  - Chapter IX – Processing Situation Provisions (Articles 85 to 91)
  - Chapter X – Delegation & Implementation Acts (Articles 92 & 93)
  - Chapter XI – Final Provisions (Articles 94 to 99)
- Supported by 2 Directives passed at the same time
  - (EU) 2016/680 Processing of personal data by competent authorities for prevention of crime
  - (EU) 2016/681 Use of passenger name records for prevention of terrorism and crime

Key aspects: security provision and key restriction

Article 5

- All personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

Article 9

- Processing of personal data revealing biometric data for the purpose of uniquely identifying a natural person, shall be prohibited.

Key aspects: Chapter III rights of data subject

Article 13

- Where personal data relating to a data subject **are collected** from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
  - List of 14 notification requirements

Article 14

- Where personal data have **not been obtained** from the data subject, the controller shall provide the data subject with the following information:
  - List of 13 notification requirements

Key aspects: information requests

Article 15

- The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
  - List of 8 requirements
- Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
- The controller shall provide a copy of the personal data undergoing processing.

Key aspects: rights to rectification & erasure (right to be forgotten)

Article 16

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

- The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay

Key aspects: rights to data portability and to object

Article 18

- The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

Article 20

- Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Key aspects: breach notification & communication

Article 33

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55

Article 34

- When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Key aspects: appointing the data protection officer (DPO)

Article 37

- The controller and the processor shall designate a data protection officer in any case where:
  - the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
  - the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
  - the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Key aspects: role of data protection officer (DPO)

Article 38

- The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. 4.5.2016 L 119/55 Official Journal of the European Union EN
- The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
- The controller and processor shall **ensure that the data protection officer does not receive any instructions** regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. **The data protection officer shall directly report to the highest management level of the controller or the processor**.
- Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
- The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
- The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Key aspects: penalties

Article 83

- Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year
  - Articles 8,11, 25-39, 42 & 43
- Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
  - Articles 5, 6, 7 & 9 – Essentially main principles for Storing, Processing or Transmitting personal data

Article 84

- Such penalties shall be effective, proportionate and dissuasive

Headlines: the basics

- Regulation – it's effective now and will become law 25th May 2018
- Guilty till proven innocent – evidence of compliance with the articles
- GDPR is already what is required – data security by design & default
- Requirement for a Data Protection Officer - independence
- Implementation will require change – impact assessments
- Member state certification & evidence of compliance shall be transparent to consumers

If you need help in understanding the impact of GDPR on your customer contact processes and need an independent DPO, then please get in touch – here to help.

John Greenwood
john@compliance3.com
+44 7767 354 354
www.compliance3.com

Compliance3
Compliant Contact Centres. *Delivered.*