GREEN 4

A guide to GDPR

AUTHOR: GREEN 4

DATE: FEBRUARY 2018

TABLE OF CONTENTS

Introduction

The General Data Protection Regulation (GDPR) will become enforceable on May 25th, 2018 and brings with it changes to Green 4's approach to data protection. The below is a summary of our stance on GDPR and some of the actions we are taking.

What is the GDPR?

By now, you will have heard of the GDPR: the General Data Protection Regulation, a European privacy law approved by the European Commission in 2016.

The GDPR is an attempt to build on and improve the current Data Protection Act and enhance individual rights and freedoms, consistent with the European understanding of privacy as a fundamental human right. The GDPR regulates, among other things, how individuals and organisations may obtain, use, store, and remove personal data.

How is the GDPR different from the current Data Protection Act? How are regulations changing?

According to the ICO:

> "Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently."

A summary of key changes are detailed below:

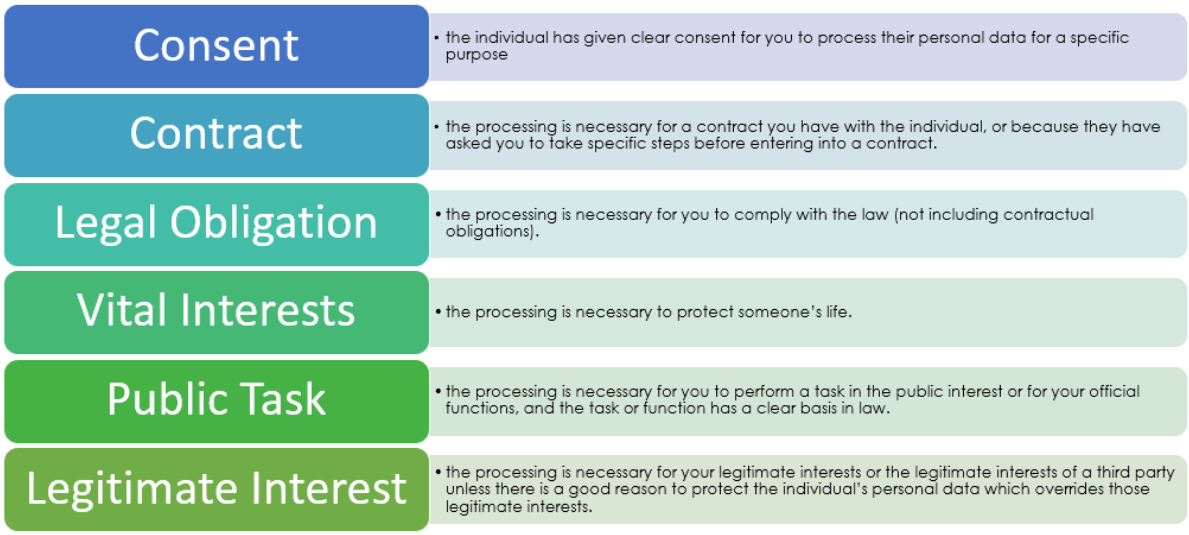
1. Expansion of individual rights

EU citizens will have several important new rights under the GDPR, including the right to be forgotten, the right to object, the right to rectification, the right of access, and the right of portability.

- Right to be forgotten: An individual may request that an organisation delete all data on that individual without undue delay.
- Right to object: An individual may prohibit certain data uses.
- Right to rectification: Individuals may request that incomplete data be completed or that incorrect data be corrected.
- Right of access: Individuals have the right to know what data about them is being processed and how.
- Right of portability: Individuals may request that personal data held by one organisation be transported to another.

2. Stricter consent requirements

Consent is one of the fundamental aspects of the GDPR, and organisations must ensure that consent is obtained in accordance with the GDPR's strict new requirements. Organisations will need to obtain consent from contacts for every usage of their personal data, unless they can rely on a separate legal basis:



3. Keep in mind that:

- Consent must be specific to distinct purposes
- Silence, pre-ticked boxes or inactivity does not constitute consent; data subjects must explicitly opt-in to the storage, use and management of their personal data.
- Separate consent must be obtained for different processing activities, which means organisations must be clear about how the data will be used when you obtain consent.

4. Stricter processing requirements

Individuals have the right to receive fair and transparent information about the processing of their personal data, including:

- Contact details for the data controller
- Purpose of the data: This should be as specific and minimised as possible. Organisations should carefully consider what data they are collecting and why and be able to validate that to a regulator
- Retention period: This should be as short as possible and reasonable
- Legal basis: Organisations cannot process personal data just because they want to. They must have a legal basis for doing so, such as where the processing is necessary to the performance of a contract, an individual has consented (see consent requirements above), or the processing is in the organisation's legitimate interest.

There are many other principles and requirements introduced by the GDPR, so it is important to review the GDPR in its entirety to ensure that you have a full understanding of its requirements and how they may apply. Green 4 recommend the Information Commissioners Office for any research or guidance (https://ico.org.uk/)

Do our customers need to comply with the GDPR?

Most likely, but this should be assessed internally with the organisations DPO, or other legal/professional advisor.

However, if you are an organisation in the EU or one that is processing the personal data of EU citizens, the GDPR will apply.

We advise our customers to consider appointing a Data Protection Officer or a GDPR owner to take ownership of GDPR (if they haven't already).

What happens if organisations do not comply?

Non-compliance with the GDPR can result in enormous financial penalties. Sanctions for non-compliance can be as high as 20 Million Euros or 4% of global annual turnover, whichever is higher.

Who are the 'controllers' and 'processors'?

If you access personal data, you do so as either a **controller** or a **processor** and there are different requirements and obligations depending on which category you are in.

A **controller** is the organisation that determines the purposes and means of processing personal data. A controller also determines the specific personal data that is collected from a data subject for processing. A **processor** is the organisation that processes the data on behalf of the controller.

The GDPR has not changed the fundamental definitions of controller and processor, but it has expanded the responsibilities of each party.

Controllers will retain primary responsibility for data protection (including, for example, the obligation to report data breaches to data protection authorities); however, the GDPR does place some direct responsibilities on the processor, as well.

In the context of the Green 4 Solutions system and our related services, in the majority of circumstances, our customers are acting as the controller. Our customers, for example, decide what information from their contacts is uploaded into their CRM system, either through a GO Booking engine, or a 3rd party data integration to capture, understand and communicate with contacts, mainly through our e-comms tool. Green 4 Solutions is acting as a processor by performing these and other services for our customers.

Will Green 4 Solutions comply with the GDPR?

At Green 4 Solutions, we believe that the GDPR is an extension of CRM best practice, and we are committed to achieving compliance with the GDPR on or before May 25, 2018.

Our GDPR preparation started more than a year ago, and as part of this process we are reviewing (and updating where necessary) our internal processes, procedures, data systems, and documentation to ensure that we are ready when the GDPR becomes effective. While much of our preparation is happening behind the scenes, we are also analysing all our current systems solutions to ensure we are able to provide the right tools to help our customers enable GDPR compliance. A summary of our process is below:

- **Data Protection Officer** – we have appointed Sam Nixon to this role. Sam is our Head of CRM, Data & Insight and a member of the Senior Management Team

- **Internal Audits** – a full data review and audit has taken place and changes made where required

- **Policies** – our company policies are being reviewed and will be updated to reflect any changes

- **Staff Training** – GDPR awareness training will be delivered to all employees at Green 4 Solutions at the next Company Meeting

How can Green 4 Solutions assist in our customers GDPR compliance efforts?

Gearing up for GDPR:

Expansion of Individual Rights

The CRM system can help promptly respond to requests from contacts:

- Right to be forgotten: Our customers may delete individual contacts upon their request at any time directly within the Dynamics CRM system (bear in mind data hierarchy challenges with 3rd party data feeds)

- Right to object: Green 4 Solutions provide web preference portals where consent can be managed by the contact directly.

- Right to rectification: Our customers may access and update your contacts within your Dynamics CRM system to correct or complete subscriber/contact information upon their request at any time. Please consider your data hierarchy and flow to make sure you are amending all relevant database (i.e. if you have a 3rd party data integration). Green 4 can help you with an internal data audit if required.

- Right of access: Our customers should consider creating or updating a Privacy Policy, ensuring it clearly describes what data collected and how it is intended to be used. The privacy policy should be available to read when a contact is considering whether to provide marketing consent.

- Right of portability: Dynamics provides an export to Excel function

Stricter Consent and Processing Requirements

Our customers must lawfully obtain and process email addresses and other personal data

• The Green 4 GO Preference portal is available to manage current customer preferences.

• There is a review of functionality of the Go preference portal and we will be releasing new features in line with GDPR:

- GDPR consent and contact consent status – applying a layer on top of existing channel consent to capture consent, or removal of consent along with a 'unknown' setting if contacts have yet to complete this information.

- Channel and preference consent – We will be including channel consent alongside existing subscriptions.
- Acceptance of privacy policy with version audit – an optional acceptance of terms section will be made available for those who wish to gain acceptance of privacy policies or other terms and conditions.

What other technology can help our customers?

At Green 4 we pride ourselves on our innovation and wide spectrum of CRM data and booking services. As a result of GDPR, we have developed a single sign on solution using OAuth industry standards that a 3rd party data capture system can hook into. This makes CRM the MASTER for capturing personal data and consent and auditing changes.

If you have specific questions about the GDPR please speak to Sam Nixon.