EFI™ WHITE PAPER SERIES

The General Data Protection Regulation (GDPR) v2.0

and EFI Solutions for eCommerce and Marketing

REVISION:
DECEMBER, 2019

Contents:

This whitepaper has been issued and approved in the English language and any translation is furnished solely for convenience. The original English text shall control and prevail in case of any variance between the English version and any translation.

1. Introduction

On May 25, 2018, a new European privacy regulation called the General Data Protection Regulation (GDPR) will come into effect. The GDPR will affect companies that accept, sell, process or store the personal data of individuals in the European Union (EU)—even if the companies or the data processing systems are not located in the EU.

This paper provides a general overview of the GDPR and the changes that may be required to systems that handle personal data, and includes specific tips for users of EFI Solutions for eCommerce and Marketing.

What is the GDPR?

The GDPR is a privacy regulation that provides individuals in the EU with greater control over their personal data and how it is collected and used. These rights apply to individuals across the EU and related obligations extend to any organizations that use or process their data, wherever those organizations are located.

Why is it important?

The GDPR gives individuals, including prospects, customers, contractors and employees, more power over their data, and restricts the ability of organizations to collect and use certain types of personal information. The regulation includes significant penalties for companies that fail to comply.

What is "personal data" under the GDPR?

"Personal data" is any information related to an identified or identifiable natural person (or 'Data Subject') that can be used to directly or indirectly identify the person. Subject to the foregoing, this includes the following types of information:

- full names
- home address
- photos of a data subject
- email address
- bank details
- online identifiers
- location details
- medical information
- computer IP addresses

Whether the information relates to an individual's private, public or work roles, it is still considered personal.

What key personal rights are protected under the GDPR?

GDPR	GUIDELINE
The right to access	Individuals can request access to their personal data, including how their data are used. The provider must provide this information free of charge.
The right to erasure, or to be "forgotten"	Individuals can, for example, withdraw their consent for the use of their personal data, and have the right to have their data deleted.
The right to data portability	Individuals have the right to receive the personal data concerning them, which they have provided to the controller. They also have the right to transmit those data to another controller without hindrance from the controller.
The right to be informed	Individuals must be informed about the use of their personal data.
The right to rectification	Individuals must be able to update and correct their personal data.
The right to restrict processing	Individuals can request that their data not be used. Subject to the GDPR, their data may remain in the company's system but not used.
The right to object	Individuals can, for example, prevent or stop the use of their data for direct marketing. This right must be made clear to individuals at the outset.

2. What does the GDPR mean to your business?

The GDPR applies to businesses and organisations that offer goods and/or services to individuals in the EU, regardless of where the data processing actually takes place. It is up to businesses and organisations to comply by May 25, 2018.

In any online system that interacts with customers, customers must be provided with the ability to agree, opt-in, or request changes, as outlined in the rights above. The business must be able to demonstrate that the customer was provided with these options and, in line with the requirement, was informed, agreed, or opted-in.

Under the GDPR "opt-in by default" is prohibited, and "pre-checked" consent boxes are not permissible. Companies may have to change their policies, processes and online systems that affect:

- online marketing and communications of all kinds
- online sales
- business processes
- applications and forms
- and more

Any personal data that are stored must have an audit trail that is time stamped. Reports must include details on how and when the contact "opted-in". The regulation also applies to purchased marketing lists.

2.1 Designing systems with "Privacy By Design"

To be compliant with the GDPR, companies must examine how they handle personal data. This may affect many systems throughout corporate departments. "Privacy By Design" is emphasised in the GDPR as a strategy for designing system-wide compliance into data processing systems.

Companies will have to explore their data archives and their policies for what data they archive, and why. They may have to put new security safeguards in place to protect against data breaches, and change policies for handling any data breaches that occur.

Companies may need new procedures for gathering and handling personal data, and for addressing consent issues so that they can prove compliance with the fundamental personal rights specified by the GDPR.

3. The GDPR and EFI's MarketDirect StoreFront and MarketDirect Cross Media

MarketDirect StoreFront is EFI's award-winning B2B and B2C eCommerce solution. It is commonly used as a Web-to-Print solution for print-related sales, but can be used to sell non-print items and support cross-media campaigns. A sample storefront can be found at http://formulaoneprint.myprintdesk.net/MarketDirect StoreFront/

MarketDirect Cross Media Marketing is a powerful tool for designing and executing high impact multi-channel marketing campaigns. These campaigns can include print, email, web landing pages, and text messages, which can be integrated with, and executed from, the MarketDirect StoreFront eCommerce site.

What kinds of data use, and what systems are affected?

Every application that collects, processes or stores personal data of individuals in the EU will be affected. Users of MarketDirect StoreFront and MarketDirect must analyze their applications for any non-compliant uses of personal data. Specifically, all user applications must provide ways for such individuals to:

- Access their personal data
- Remove consent/request deletion of their data
- Request transfer of their personal data from one provider to another
- "Opt-in" before data are collected as required by the GDPR
- Correct/update their personal data
- Request their personal data not be used
- Prevent their personal data from being used in marketing

For new applications, the principles of "Privacy by Design" should be built-in to ensure compliance.

For existing applications, applications should be analyzed for:

- **Wherever personal data are requested and collected**
  New "opt-in" provisions should be added, with clear explanations of how personal data are handled. New options for individuals to request access/make corrections/change usage/delete their data should be added.
- **Where data is stored, processed and transferred**
  GDPR protocols should be followed.
- **Data breach detection**
  The ability to notify affected data subjects where required by the GDPR.

4. MarketDirect StoreFront and the GDPR

MarketDirect StoreFront is available as a self-hosted solution, in which the user stores the system (and all personal data) on-site. It is also available as a cloud-based solution, which stores personal data in the cloud in the EFI hosting center in Pittsburgh, PA, USA hosting center, or its UK hosting center using Amazon Web Services (AWS)..

In both options personal data and consumer data (related to orders) are stored:

- Personal data is stored in a user profile, which includes name, email, phone, address, and (for business customers) cost center
- Consumers can upload data lists which could contain any information
  That list is associated to an order and can be re-used in subsequent orders
- Consumers can upload artwork/text that could contain any information
  This artwork is associated to an order and can be re-used in subsequent orders

In the cloud-based option, hosted data are backed up daily and stored for 28 days.
Customers do not have access to these backups without the involvement of EFI, the server provider.

4.1 Strategies for compliance

4.1.1 Create custom terms and conditions that explain how personal data will be used

With MarketDirect StoreFront, you can create your own clearly worded terms and conditions for users, that explain how their data will be used. Choose ***Administration>Language Management*** and click ***Customize Settings,*** then enter the custom terms and conditions.

Your unique terms and conditions will be viewed when a user creates an account, and on any page via the terms and conditions link.

4.1.2 Allow your buyers to access their data

MarketDirect StoreFront provides your buyers with access to their order history whenever they are logged in. ***Order History*** is in the dropdown from the buyer's name, generally in the upper right corner of the page. If a buyer needs help finding their Order History, instructions are available if they search the online help.

Developers could optionally enhance the experience by adding the ability to ***Export Order History*** (as a CSV file) to the Order History screen.

4.1.3 Provide buyers with access to their data (in an easy to read, machine-readable format)

Administrators can provide customers with reports of their personal data. In the ***Reports*** section of *Administration:*

- *Revenue and Invoices by User* is accessed under *Financial Reports*
- *Order History by User* is accessed under *Production Reports*

If a customer requests specific information, Administrators can create custom reports, using the Dynamic Query Tool for any field of data in MarketDirect StoreFront.

4.1.4 Allow buyers to be "forgotten"

Data erasure is possible, by contacting EFI support (MDSF.support@efi.com). Should a customer request to be forgotten and to have their data purged, EFI will execute a script that anonymizes customer contact details and Delivery Contact details, and deletes any stored content files including Customer Profile data.

- **Customer Profile** data is application-dependent; it is typically used to prepopulate some personalized products, and to identify the buyer and their preferences. It could include nickname, first/middle/last name, title, company, address, phone, and email
- **Content Files** are files uploaded by customers for their print and associated jobs, including for personalized products. These files will expire and be purged automatically (based on the application's settings). Content files could include:
  - PDF, Word, PowerPoint, image files, or other digital content
  - Image and text files for variable-data or personalized products
  - Mailing lists for variable-data mailouts
- **Delivery Contact** details are used for shipping and delivery, and can include: recipient first/middle/last name, address, company, phone, and email

5. MarketDirect Cross Media and the GDPR

MarketDirect Cross Media is available as a self-hosted solution, in which the user stores the system (and all personal data) on-site. It is also available as a cloud-based solution, which stores data in the cloud in the EFI hosting center in Pittsburgh, PA, USA hosting center.

In the cloud-based option, hosted data are backed up daily and stored for 28 days. Customers do not have access to these backups without the involvement of EFI, the server provider.

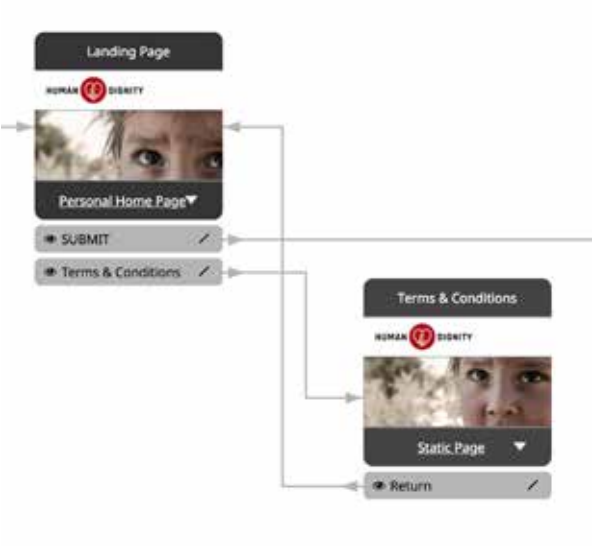
Campaigns may collect and store personal data, such as name, address, email, phone, etc., and may collect any kind of data through website forms. Campaigns may also track and store visitors' website visits via cookie tracking. The nature of the data that are collected by, and used within a Cross Media campaign is completely dependent on the application, and the requirements of the user's marketing campaign. EFI has no knowledge of or control over these data.

5.1 Strategies for compliance

5.1.1 Clearly communicate terms and conditions

Your campaign must make it clear to any site visitor what information is being captured by visiting your page(s), whether they visit a pURL or fill in a form with personal data (as defined by the GDPR). The information must clear and easy to understand.

To do this, place your terms and conditions directly on the page, or include a link on every campaign page that points to a static terms and conditions page. Be sure to save the fact that the visitor clicked on terms and conditions, as a user action in the database.



	xmediaID	LpLogin	DSM_LeadScore	Salutation	FirstName	LastName	EMail
	17	john1470	10	Mr.	John	Doe	john@doe.com

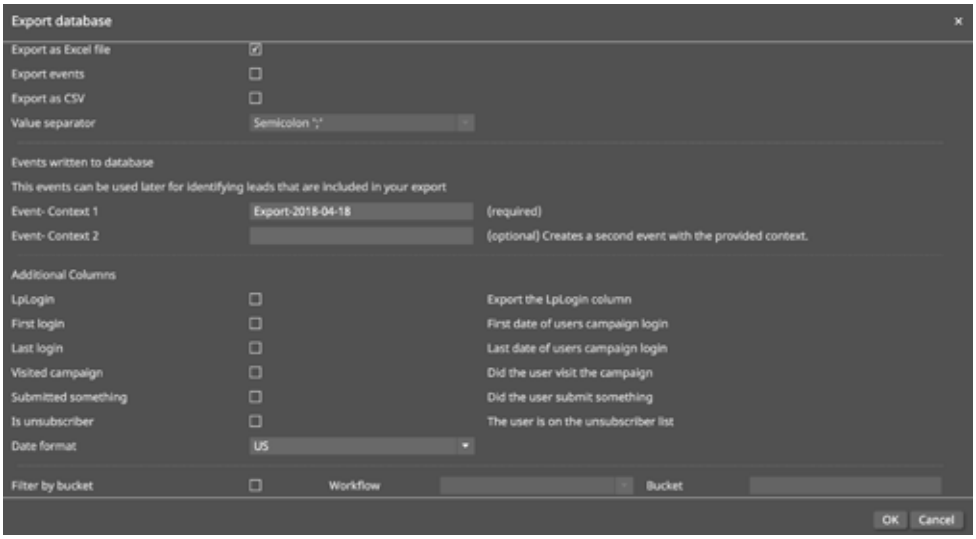
Page 1 of 1 (5 events total)

Id	OccuredOn	CampaignName	EventType	Context	Destination
459	2018-04-18T19:51:09.703Z	SpecialOffer	Visited	TermsConditions.html	
458	2018-04-18T19:51:09.690Z	SpecialOffer	Login		

5.1.2 Allow participants access to their personal data

A campaign's designer can easily access campaign data through the Database icon. The data can be filtered by the participant name or other data field, and exported as an Excel file.

A database export can be filtered by creating a workflow bucket with a Contains or Equals filter equal to the participant's name. Select ***Filter by Bucket*** and the appropriate bucket, to export the participant data and all data points that the participant accessed in the campaign. Exporting the filtered list and providing to the individual may materially satisfy the Accessibility and Portability requirements of GDPR.



5.1.3 Allow a campaign participant to be "forgotten"

To "forget" a campaign participant, go into each campaign database, then select and delete the participant's record. This will remove the participant from every campaign using that database. If a participant's data is in multiple databases, they will have to be deleted from each database.

Disclaimer: MarketDirect StoreFront and MarketDirect Cross Media Marketing are development tools. Issues of GDPR compliance are the responsibility of the application developers. This paper provides general guidelines only, and does not assure compliance or constitute legal advice.

EFI fuels success.

We develop breakthrough technologies for the manufacturing of signage, packaging, textiles, ceramic tiles, and personalised documents, with a wide range of printers, inks, digital front ends, and a comprehensive business and production workflow suite that transforms and streamlines the entire production process, increasing your competitiveness and boosting productivity. Visit www.efi.com or call 0808 101 3484 (UK only) or +44 (0)1246 298000 for more information.

GVP.031.12.19 UK