



CAPTIVAPOS

General GDPR Guidelines.

GDPR and Captiva Systems.

May 25th 2018 sees the introduction of GDPR in Europe.

To improve the manageability of GDPR data in your Captiva systems and to help you respond to customer queries, we have included in the latest versions some tools to help you comply with GDPR regulations.

Customers with valid service accounts will be automatically contacted over the coming weeks and offered the update free of charge. If you do not have a valid service account charges may apply.

Does this mean that our system is not compliant until the upgrade?

No, not necessarily, you can continue to use your systems as normal, but you should plan to update to the latest versions. It really depends upon the nature of your business. You should review how you use customer data (exporting etc.), and we recommend you review your security settings and user permissions. Take a look at "some basic guidelines" below and take any steps that may be relevant to your business.

Please note that Visual POS version 4 has not been supported for a number of years now. If you have not updated in a long time you may need an update.

In order to continue full compliance we recommend that users always keep their systems protected with the latest versions of Visual POS, operating systems, malware protection and backups.

Customers should update to the latest version at the earliest convenience.

What will change on 25th May 2018?

In order to ensure compliance, there are two areas of our systems where changes will come into force on the 25th May 2018.

1. From 25th May 2018 our systems will not process SMS campaigns that have been sent by versions earlier than version 5800.
2. From 25th May 2018 third party services that access your data via our API's will need to have a data profile setup. This allows you to control what data is being accessed. For example: a stock controller who accesses sales information via API can potentially see customer data. From 25th May 2018 they will no longer see this data unless you explicitly give consent.

What's in the latest version?

Tools to easily identify when GDPR is used on receipts and printouts.

Tools to secure the data on your system.

Better tools to control access to sensitive data.

Utilities to enhance data housekeeping.

Some basic guidelines.

You should be mindful of GDPR requirements with any information exported from your system. Use user permissions to control access to GDPR sensitive areas.

You should review your receipts to determine if any personal customer data is being used, and if so, is it necessary. For example; does a customer phone number need to be printed on a kitchen ticket? You can manage the information displayed on tickets using system setup. Version 5800 onwards has features to easily identify when a receipt or print out contains personal data.

You should review customer data and remove older data that is no longer required or has expired.

You should avoid submitting SMS marketing campaigns until you upgrade to 5800 or later. Messages sent using older versions will not be sent if you do.

If you do so, you should review any information you share via our API with any external companies, such as stock controllers, business intelligence systems, delivery service providers.

In general you should ensure that those companies are

- only processing data required to full fill the service they have been employed to process,
- that they are not unnecessarily retaining the data for longer than necessary,
- that they are not using the data for other purposes,
- that they are not sharing the data with any other parties / sub-contractors without consent.

From www.dataprotection.ie :Business Contacts (Customers and non Customers)

Source: <https://www.dataprotection.ie/docs/DIRECT-MARKETING-A-GENERAL-GUIDE-FOR-DATA-CONTROLLERS/905.htm>

You may not use electronic mail to send a marketing message to a business contact address/number if the subscriber has notified you that they do not consent to the receipt of such communications.

SUMMARY

The following table summarises the rules that apply.

	Postal Marketing	Text/Email Marketing	Phone Marketing to Landlines	Fax Marketing	Phone Marketing to Mobile Phones
Individual Customer	Opt-Out**	Opt-Out** (provided similar product or service)	Opt-Out**	Opt-Out**	Opt-Out**
Individual Non-Customer	Opt-Out**	Opt-In*	Opt-In* if on NDD, Opt-Out** otherwise	Opt-In*	Opt-In*
Business Contacts (Customer & Non-Customer)	Opt-Out**	Opt-Out**	Opt-In* if on NDD, Opt-Out** otherwise	Opt-In* if on NDD, Opt-Out** otherwise	Opt-In*

- *Opt-in means you can only market an individual where you have their explicit consent to do so. Similarly, selected third parties with whom you share your marketing lists may only market an individual where you have obtained the explicit consent by the individual for marketing by each specific third party.
- **Opt-out means that you can market an individual provided you have previously given them the option not to receive such marketing and they have not availed of this option.
- For all Electronic Marketing Communications, an option to unsubscribe must be included.

Some general non-Captiva guidelines...

You should have produced a Privacy Impact Assessment for your business.

You should have a privacy statement on your website if relevant.

You should have a "we use cookies" notice on your website if you use them.

Good to know...

Over the past year we have been updating our cloud systems to ensure the highest standards and latest versions are in place.

Data transferred via our API's and systems have always been over secure https connections.

Our cloud services have the latest patches applied automatically as providers make them available.

Our SMS services have always included a free, easy to use opt out service. Free text back.

We adopt a privacy by default approach to GDPR.

Should you receive any “freedom of information” requests we are happy to assist.

Visual POS already has features to record customer consent.

We do not save any customer credit/debit card information.

We do not record customer date of birth, mother’s maiden name or other security questions.

We do not employ and third parties to analyse your data.

Further reading.

We have found the following resources helpful in understanding GDPR.

Websites:

<https://www.dataprotection.ie/docs/Contacting-Customers/1248.htm>

Legislation: <https://gdpr-info.eu/art-27-gdpr/>

GDPR informer: <https://gdprinformer.com/getting-started-with-the-gdpr>

Apps:

GDPR Ireland by A&L Goodbody

<https://itunes.apple.com/ie/app/gdpr-ireland/id589404330?mt=8>