
iconsent
by eDynamix
A universal GDPR solution for the Automotive Industry

iConsent

Capture and store all your consent in one place using iConsent. Available for both tablet and desktop, iConsent is fully embedded within the eDynamix platform with optional DMS integration*. With real-time reporting via the Connect App** and regular reports pushed to your email, iConsent also comes with our GDPR Cleanse module to aid in GDPR compliant marketing.

Service Plan

- When creating a quote, iConsent will check existing consent and prompt either the user to obtain or customer to provide where missing

Online Bookings

- When creating a booking, iConsent will check existing consent and where missing, will ask the customer to complete their marketing preferences

Sales Desk

- When creating an enquiry, iConsent will check existing consent and prompt the Sales Executive to obtain from the customer where missing

iVHC

- When checking a customer in, iConsent will check existing consent and prompt the Service Advisor to obtain from the customer where missing

automate**

- Customers using the app will be periodically prompted for consent where missing

Complete logging of Consent details include:

- User & method of capture
- Time & date
- Privacy Policy version

*DMS Dependant **Coming soon

GDPR Cleanse

GDPR Cleanse provides a mechanism for full GDPR compliance when marketing your customers once consent has been captured using iConsent. GDPR Cleanse works with any DMS* without the need for full integration and is equipped with a SAR Console for easy handling of Subject Access Requests. Right to be forgotten management and full integration to the Telephone and Mail preference services can also be included for efficient removal of customer data on the eDynamix platform.

Follow Up

- Maintenance reminders sent in accordance with consent options
- Marketing and non-marketing reminder options available
- User prompt when booking if no consent for customer

Reporting

- Comprehensive desktop suite of reports to analyse consent, SAR requests, RTBF requests, etc.
- Regular push reporting of key information

Connect

- iConsent captured data can be analysed in our Connect management app
- Available to all iConsent customers

Allowing easy cross referencing of database extracts with consent recorded via iConsent in 4 easy steps:

- Export marketing database from the DMS
- Upload to GDPR Cleanse
- Compare with iConsent including consent breakdown analysis by contact method
- Download the cleansed file ready for marketing

*Export format dependant

Pricing

iConsent

£99 per month, per dealership which includes the following:

iConsent Tablet & Desktop Applications
iConsent integration with the following eDynamix Modules:

- iVHC
- Sales Desk
- Service Plan
- Follow Up
- Online Booking
- automate customer app

GDPR Cleanse
MPS & TPS Integration
Automatic email validation
Privacy Policy Management
Connect App Reporting

DMS Integration

From free (DMS dependant)

General Data Protection Regulation (GDPR)

Ensure that all your systems, processes and suppliers comply with the requirements now and in the future to avoid very large fines.

The overview

The General Data Protection Regulation (GDPR) is a new set of rules governing the privacy and security of personal data laid down by the European Commission. It will ensure that all countries in the EU, and those companies using personal data for EU citizens, adhere to the same data protection rules. It will regulate details such as the user data that companies are allowed to collect, how it is stored, how data breaches can be safeguarded, whose responsibility it is in the event of a breach, and also the inherent sanctions.

To put it simply, it is the biggest change in data protection laws for 20 years which could have far-reaching, and potentially damaging consequences for businesses.

The legislation presents a range of compliance and operational challenges for businesses, requiring thorough planning and additional resources.

The definitions

Data processors.
A data processor is an organisation that processes data on behalf of data controllers e.g. cloud service providers.

Data controllers.
A data controller is an organisation that collects data from data subjects.

Data subject.
A data subject is any EU citizen (an individual) for which personal data is recorded.

Personal data.
Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, telephone number, a home address, a photo, an email address, bank details, posts on social networking websites, medical information or a computer's IP address.

The questions

If you answer "No" or "I don't know" to any of the questions below, please get in touch with us so we can help you on your journey towards the GDPR compliance.

- Are all your suppliers who handle your customer data ISO 27001 compliant?
- Do you collect personal data and know what it is used for?
- Do you have a mechanism to ask for consent?
- Do you have a mechanism to record consent?
- Do you have a process to record who has given consent and retrieve what consent they have given?
- Can you give your customers the option to "opt out" or unsubscribe electronically to future marketing?
- Do you have an option to "opt out" or unsubscribe to printed mailers?
- Do you have a mechanism to record who has requested to "opt out" or unsubscribe so you stop sending information?
- Can a customer easily gain access to all the information you hold on them?
- Can a customer easily update their information in all your systems?
- Do you know where the personal data you hold is stored?
- Do you know how long you store personal data for?
- Do you know who within the organisation has access to the personal information you store?
- Do you destroy your data at the end of the contract with the customer?
- Do you know how this data is destroyed?
- Do you have a centralised and consistent privacy policy that is compliant with the GDPR?

The facts

- The GDPR replaces the outdated Data Protection Directive (1995.)
- It will contain many of the same principles and concepts as the current Data Protection Act (1998), although there are many new elements and some significant enhancements.
- It comes into effect on May 25th, 2018.
- It is one set of laws that apply across all 28 EU member states.
- The UK will still adopt and mirror the legislation even after Brexit.
- It applies to any organisation outside the Union when processing the data of citizens within it.
- The ICO can issue very large fines on any company that fails to comply with the legislation.

The purpose

- The GDPR is intended to give control back to people over the use of their personal data.
- It strengthens the rules for obtaining consent.
- It strengthens the need for breach notifications.
- It emphasises self-assessment in the management of data.
- It places greater emphasis on the documentation that data controllers must keep.
- It requires that data controllers are able to demonstrate their accountability.
- It will help with the flow of data between the UK and the EU post-Brexit.

The GDPR rights

The right to be informed
This emphasises the need for transparency and the requirement to inform the customer how you will use their data, typically through a privacy notice.

The right to restrict processing
An individual can request that you no longer process their data but still store it. Just enough information about the individual must be retained to ensure that the restriction is respected in future.

The right to object
Individuals can object to you processing their personal data unless you can demonstrate compelling legitimate grounds for doing so which outweigh their interests, rights and freedoms, or if the processing is required as part of a legal claim. However, you must stop all processing, at no cost to the individual, if the data is being used for direct marketing.

The right of access
This right allows individuals to access the personal data you hold on them and confirmation of how and why it is being used.

The right to data portability
This allows individuals to gather and easily, safely and securely move, copy or transfer their personal data for their own purposes across different IT services and environments without impacting its usability.

The right not to be subject to automated decision-making including profiling
Individuals can request that their personal data is not used where automated decisions which potentially have a damaging legal or similar effect on them are made using this data without some form of human intervention.

The right to erasure
Also known as 'the right to be forgotten', this principle allows an individual to request the deletion or removal of their personal data without specifying a reason for the request.

The right to rectification
This means that individuals can request that any inaccurate or incomplete personal data you hold on them must be rectified. If any of their data has been shared with third parties, they too should be informed of the rectification. You must also inform the individuals, where appropriate, about the third parties with which their data has been shared.

The requirements

Consent

- The exact use of the data that is being consented to must be granular, simple to understand and communicated in clear terminology.
- Consent must also be auditable whereby data controllers can prove the "consent" (opt-in.)
- Consent requests must be separate to all other terms and conditions.
- Consent cannot be used as a prerequisite to gain access to any services.
- It must be easy for a data subject to withdraw consent.
- You must inform individuals of their right to object "at the point of first communication" and also in your privacy notice.
- Organisations must also protect individuals' right to be forgotten when their data is no longer relevant or necessary.
- It should be easy for an individual to move, copy or transfer their personal data across different services.
- This data must be provided within one month of it being requested, and may also need to transfer it directly to another organisation if this is feasible. It must be done free of charge and in a common, structured and machine-readable format.

Documentation

- Formal Data Privacy Impact Assessments (DPIAs) are required when using new technologies and for any data deemed "high risk" to the rights and freedoms of individuals.
- Internal records must be kept of all data processing activities, with the data tagged and classified.
- Data processing privacy policies and practices should be reviewed as processors are now subject to GDPR obligations.
- A clear and complete Data Privacy Notice is important for handling personal data, for instance if a dealer is collecting data for another party, it has to be made clear and agreed to by the customer.
- The data controller should implement measures which meet the principles of data protection by design and data protection by default.
- It is the responsibility and liability of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller.
- Data Protection Impact Assessments have to be conducted when specific risks occur to the rights and freedoms of data subjects.
- Records of processing activities must be maintained, that include purposes of the processing, categories involved with envisaged time limits and must be made available to the supervisory authority on request.
- Organisations must be able to show how they comply with the data protection principles in their business processes for products and services.

Breaches

- Data controllers must notify data protection authorities of any breach that risks the rights of individuals within 72 hours of them becoming aware of it.
- Individuals, where a high-risk breach could affect their rights and freedoms, must be notified as soon as possible.
- When a data processor discovers a breach, it is their responsibility to notify the controller.
- Reporting a personal data breach to the ICO is required if it is likely to result in a risk to the rights and freedoms of individuals, such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Data protection officer

It is recommended that businesses designate a Data Protection Officer (DPO) to ensure all data processing operations are compliant.

The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data.

The DPO will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organisation that employs them.

CAS

The eDynamix Consent Authorisation Server (CAS) provides a mechanism for capturing and storing consent from customers while not allowing any communication to be sent to those where consent has not been gained, helping dealers maintain compliance to the GDPR.

Digital Consent

Customers are required to explicitly select and consent to all forms of communication that are sent from a business with a digital signature taken and stored against the consent record.

Privacy Policy

A centralised privacy policy should be available to customers across all platforms and, when modifications are made, should be available in all locations.

Whitelist

The whitelist will ensure that no electronic communication is sent from the business to a customer who has not consented to have their contact details recorded, receive emails, SMS, telephone calls or direct mail.

Multiple Systems

Systems together with a dealers DMS system can feed into and read from the CAS to ensure customer contact preferences are maintained and communication cannot be sent without explicit consent.

t: 0845 413 0000
e: enquiries@edynamix.com
find us on Twitter, Facebook and LinkedIn

eDynamix

LLOYD'S REGISTER · LRQA
ISO/IEC 27001