General Data Protection Regulation (GDPR) & Ruler Analytics - Overview

Intro & Disclaimer

The General Data Protection Regulation (GDPR) is new legislation that comes into effect on the 25 May 2018. It replaces the Data Protection Act of 1998 (the "DPA").

This document is a summary of GDPR and implications for the use of Ruler Analytics.

A quick disclaimer, this document does not constitute legal advice, this information is for guidance purposes only, you should seek your own legal advice to ensure you comply with the GDPR.

Overview of GDPR

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 so you will have to do some things for the first time and some things differently.

You may use our checklist below but we recommend you seek independent legal advice and also use the checklists and other Information Commissioner's Office (ICO) resources to work out what you need to do to ensure you comply with the GDPR. (www.ico.org.uk)

The GDPR places greater emphasis on the documentation that data controllers and processors must keep demonstrating their accountability.

Who does the GDPR apply to?

- The GDPR applies to 'controllers' and 'processors'. Ruler Analytics ("us", "we", "our" "Ruler") is a processor and our clients ("you", "your", "client") are controllers.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- The GDPR places specific legal obligations on us as processors and, as the controller, you are not relieved of your obligations just because we have been instructed to process your data. The GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. So, for this purpose we need to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities as set out under the GDPR. We must only act on the documented instructions of a controller and it's important we document those instructions as set out in our

written contract and are comfortable with the extent to which we are requested to conduct the processing accordingly.
- So, for the reasons set out above, we require you to accept our terms before we commence our processing services

What information does the GDPR apply to?

Personal data

As with the DPA the GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Personal information that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Equally behavioural information which when tagged together with other personal information related to an individual which may be used to identify a person may also fall within the definition of personal data. This might include information which makes up the profile or a person and their buying habits.

Anonymous / Hashed Option

Ruler Analytics will offer an anonymous / hashed version of the product where all PII (Personal Identifiable Information) is hidden within reporting and replaced by hashes. This does not bypass GDPR as we still process the e-mail or phone number at the point of entry; it will, however, improve the confidential nature of the personal information.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data"

As well as the same categories of sensitive data under the DPA the special categories under the GDPR specifically include genetic data, and biometric data where processed to uniquely identify an individual.

For the purposes of this quick guide and our contracts with clients we assume the client shall not instruct us to process special category data.

Your customer's rights as individuals

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some enhancements. You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Obligation on you to notify your customers and visitors of their rights

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. This may include the way in which we are processing that data on your behalf.

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing. You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA but there are much stricter rules which apply to the use of consent. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. You should read the detailed guidance the ICO has published on consent under the GDPR, and use their consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.

It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent.

Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. The GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'. This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

Obligations to report data breaches

We are both expected to put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred.

Lawful Bases and Legitimate Interest

We take very seriously the issue of privacy and confidentiality. For the purposes of GDPR and our contract with you we consider you (our client) are the data controller of your own and your customer/visitor personal data and we are the data processor.

As the data controller you are responsible for determining how and why (being the purpose) the personal data is collected.

As you have entered into a contract with us to act as your data processor we shall collect and process the personal data on your behalf strictly in accordance with your instructions under our agreement. As you are aware both data controllers and processors have separate legal obligations and duties under GDPR to ensure personal data is processed in compliance with all applicable data protection legislation.

In order to collect and use personal data, the data controller determines how it is collected and processed so you must ensure you have established and can demonstrate which lawful basis you are relying on for such intended use or processing.

To help you decide on what lawful basis is appropriate we have set out below our thoughts on the issue.

We have considered our own position with regard to the instructions you provide and we are reliant on your decision as to the lawful basis you have determined as per our contract terms. Therefore, we have entered into that contract on the understanding we will process the personal data we collect for you based on your instructions. As the data processor we are obliged to follow your instructions to fulfil our obligations under the contract unless we consider the same to be unlawful in which case we will notify you.

So, you also need to inform your customers or users of your service that whenever they provide you or us with their personal data you have clearly and fairly explained to them what personal data is being collected, why it is being processed and who is doing the processing and the legal basis you (the controller) is relying on to do so.

The GDPR requires the relationship between the controller and processor to be in writing and contain mandatory data processing clauses. Therefore, we have updated our terms and conditions with the appropriate data processing clauses which will form our new agreement.

Clearly, as you'd expect, your privacy policies and notices are your affair, are specific to you and you are responsible for ensuring they comply with the law and notify each customer and visitor of how we are collecting and processing their data on your behalf. To help you in determining the lawful basis for processing your customers' or visitors' data we would suggest you consider the following:

1. When we collect an individual's email we simply match it to the marketing source that drove the individual to respond. We do not access any other personal data and we simply pass that information onto you so you can see how well a marketing campaign had worked in generating sales. We would suggest this is a legitimate interest of yours and on the balance of interests in the mind of the individual would not be an unexpected consequence.
2. Equally when we record the telephone number and link that with a number used to demonstrate a sales and marketing campaign that too would be a

legitimate interest of yours and we would anticipate this again would be a reasonable expectation of the individual caller.

3. The above all assume you do not then use that personal data for any other purposes.

It is therefore important to thoroughly assess upfront which basis is appropriate and document this. It may be possible that more than one basis applies to the processing because you have more than one purpose, and if this is the case then you should make this clear from the start.

As with any contract, policy or guideline we would recommend you seek independent legal advice before you act upon any of these tips and guidelines. Ruler Analytics are not lawyers and we do not purport to advise clients in that guise. We disclaim any liability for any costs, loss or damage you suffer as a consequence of following any of the above.”

Implications

Implication: does the reason for processing the data fall within one of the lawful bases under GDPR?

Under the GDPR it is your responsibility to ensure the collection and processing of data is done legitimately under one or more lawful bases. Our terms require you to confirm you have the ensured that the processing we conduct in accordance with your instructions complies with one of the lawful bases under the GDPR.

In the context of collecting and processing data for marketing purposes our clients have in the past tended to rely on consent or legitimate interests as the lawful basis for such processing. These principles haven't changed but GDPR has changed the application of both bases.

Consent

The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Clients are advised to keep clear records to demonstrate consent.

The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

Legitimate interests

If you are relying on legitimate interest basis, the biggest change is that you need to document your decisions on legitimate interests so that you can demonstrate compliance under the new GDPR accountability principle. You must also include more information in your privacy notice.

We recommend, in the run up to 25 May 2018, you review your existing processing to identify your lawful basis and document where you rely on legitimate interests, update your privacy notice, and communicate it to your customers.

Implication: Right of Access

Individuals have the right to access their personal data and supplementary information.

Not only may individuals request such information from you but may also request the same directly from us and we will need to comply as the data processor.

In general, the information must be provided free of charge and within a month.

There are exceptions for complex and vexatious requests.

Implication: Right of Rectification

Your customers may request us directly to rectify any data held by us about them. We must do so within one month of the request and will notify you of the same.

Implication: Right to Object

Individuals have the right to object to:

- processing based on legitimate interests; and
- direct marketing (including profiling);

If applicable, your customers may request us directly to stop processing their data at anytime.

You must inform individuals of their right to object “at the point of first communication” and in your privacy notice.

Implication: Ruler Processing Form Submissions

Based on your specific requirements Ruler collects the personal information of individuals who visit your website via form submissions placed by us on your website such as name, e-mail, phone number etc. You are able to select the fields you wish to collect and not collect. Ruler processes this data and matches it with marketing source and page journey information for marketing measurement purposes.

Make sure your terms of service or privacy policies/notices effectively inform your users how you are using Ruler Analytics (and any other similar services) on your website or app. This requirement has always been part of our Terms of Business, but the GDPR requires this is done more specifically and clearly. We recommend you ensure your policies are up to date and clear to your readers to inform them that data is processed for marketing measurement purposes.

Implication: Ruler Processing Phone Numbers

Ruler captures inbound phone numbers from phone calls. Ruler processes this data and matches it with marketing source and page journey information for marketing measurement purposes.

Make sure your terms of service or privacy policies/notices effectively inform your users how you are using Ruler Analytics (and any other similar services) on your website or app. This requirement has always been part of our Terms of Business, but the GDPR requires this is done more specifically and clearly. We recommend you ensure your policies are up to date and clear to your readers to inform them that data is processed for marketing measurement purposes.

Implication: Ruler Processing Phone Call Recordings

Ruler has an option of whether to record phone calls or not, you can stipulate whether you want this feature to be enabled. We are also able to include an initial greeting of your choice to inform the caller that calls are recorded. The purpose calls are recorded depends on your instruction. In the main, we understand the primary purpose is to assess the quality of a lead.

Implication: Retention of Data

In accordance with the GDPR we are only permitted to retain data for as long as is necessary for the purpose for which it is collected. In general, we consider all data should not be held for longer than 1 year to allow you a reasonable time to collate and process the results of our processing services. If you would like the data to be held for a longer or shorter period of time we offer you the ability to tell us and provide us with the justification for doing so before we alter the period.

Implication: Location of data

All of the data we collect is hosted within the EU and will continue to be unless notified otherwise.

Implication: Data should be deleted or ported if needed / right to be forgotten

Data subjects have the right to be forgotten or transferred to another entity and as a consequence may request directly to us that their data is deleted or ported by us.

Equally, we do the same if you have the consent of the data subject to do so.

Contact Us

With regard to any of the above information please contact us for information on info@ruleranalytics.com