Tag Inspector
AN INFOTRUST PRODUCT

EVERYTHING MARKETING & ADVERTISING PROFESSIONALS NEED TO KNOW ABOUT GDPR

General Data Protection Regulation (GDPR)

THE MATERIALS ARE PROVIDED **AS IS** WITHOUT ANY WARRANTY AND INFOTRUST, LLC DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, REGARDING THESE MATERIALS. THE INFORMATION CONTAINED IN THESE MATERIALS WAS PREPARED FOR GENERAL INFORMATIONAL PURPOSES AND IT IS NOT INTENDED TO PROVIDE LEGAL ADVICE. BEFORE APPLYING ANY OF THE INFORMATION TO YOUR SITUATION, YOU SHOULD CONSULT YOUR LEGAL ADVISORS

Tag Inspector
AN INFOTRUST PRODUCT

TABLE OF CONTENTS

GDPR

Regulations vs. Directives

Regulations are the law, as it is written. The General Data Protection Regulation **(GDPR)** falls into this category, applying to all EU-member states, with **the goal of protecting the fundamental rights of individuals as it pertains to data collection and data processing**.

Directives are special and specific, providing guidance for staying within the law. Rather than applying blanket guidance, these are provided by individual EU-member states, which means that there is variation in the direction they provide. The **ePrivacy** directive is a good example of this, **providing specific guidance on marketing activities across a broad range of technologies and circumstances**.

GDPR

Type: Regulation

What It Does:
Protects the person and their fundamental human rights.

ePrivacy

Type: Directive

What It Does:
Protects specific pieces of information: An email address and cookies.

An Overview of GDPR

Intent

Instill basic privacy rights as human rights, as it pertains to personal data.

Purpose

To force organizations to think about privacy and put privacy practices in place for all data collection activities.

Fines

There are two types of infractions, each with their own punishment or fine.

- ***Failure to Notify of Breach:***
  Up to 10 million Euros or 2% of annual global revenue (whichever is higher)
- ***Processing and Failure to Protect Human Rights:***
  Up to 20 million Euros or 4% of annual global revenue (whichever is higher)

Note that if an individual can prove negative impact as a result of how data was collected or used, they have a right to file a compensation claim against an organization.

Consideration

The nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them will be taken into consideration when assessing fines.

Important Definitions

Controller

Determines the purposes and means of processing personal data. This is the organization determining:

- *What platforms are used for marketing, analytics and advertising*
- *What data is collected*
- *Architecture for how data is being collected*
- *How collected data will be used*

Processor

Responsible for processing personal data on behalf of a controller.

Personal Data

Any information that can be used to directly or indirectly identify the identity of a natural person.

Processing

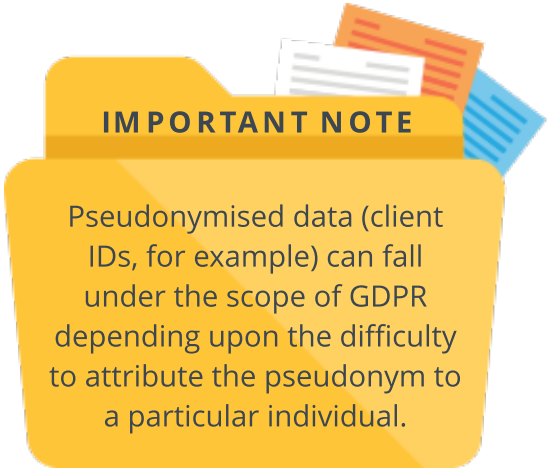
Any operation performed on personal data or on sets of personal data. Processing includes actions such as:

- *Retrieving information in a spreadsheet*
- *Creating a report*
- *Setting up a tag architecture for data collection*

EXAMPLE: USING GOOGLE ANALYTICS

CONTROLLER: YOU

PROCESSOR: GOOGLE



Who Does GDPR Apply To?

GDPR is a European Union initiative. As such, its concern focuses on data subjects (people) within the EU.

This means that the **GDPR** applies to you if:

You are an organization operating within the EU.

You are an organization offering goods or services to subjects within the EU.

THE SIX PRINCIPLES OF GDPR

Personal Data Shall Be:

"Processed lawfully, fairly, and in a transparent manner..."

- **Lawful:** You need to have a legal basis for processing information.
- **Fair:** The result of collecting and processing the data must not cause damage to the subject.
- **Transparent:** The individual needs to have visibility into the processing of their data.
  - What data is collected?
  - Why is it collected?
  - What is the end result of collecting the data?

"Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for... statistical purposes shall not be considered to be incompatible with the initial purposes"

- **Specified:** Data must be used for the explicit reason for which it is collected.
- **Explicit:** Must define an explicit reason for collecting and processing personal data; it must only be used for this stated purpose.

Personal Data Shall Be:

"Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed"

- **Adequate + Limited:** You must collect only the minimum amount of personal data necessary in order to be able to accomplish your stated purpose.
- **Relevant:** The data must be relevant within the context of the stated purpose.

"Accurate and, where necessary, kept up to date" - "every reasonable step must be taken" inaccuracies be erased or rectified without delay.

- **Accurate:** Data must be accurate and clean.
- **Inaccuracies:** In the event an inaccuracy is detected, it must be erased or rectified immediately.
    - If you share data with other processors or controllers, they must be notified of the inaccuracy so that they can also update the record.

Personal Data Shall Be:

"Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"

- **No Longer Than Necessary:** Data can only be kept for the amount of time necessary.
- **Permits Identification:** If the information is identifiable, and must remain so for the stated purpose, it must be obfuscated or deleted as soon as the processing is complete.

"Processed in a manner that ensures appropriate security of the personal data... using appropriate technical or organizational measures"

- **Security:** You must have internal processes in place to protect the personal data of individuals.
- **Technical or Organizational:** The processes can be administrative as well as technical.

Summary

Whenever you are dealing with personal data, use these as your guiding principles:

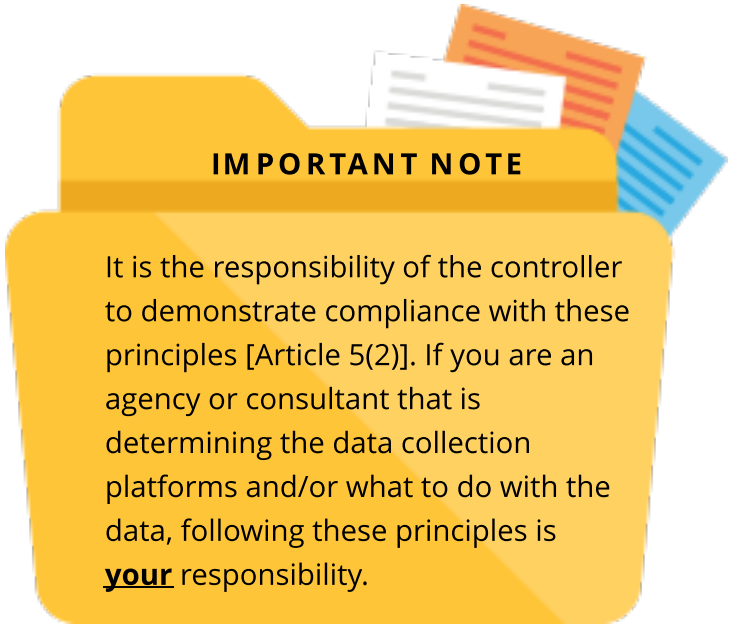
Personal data should be collected for a specific, legitimate purpose.

Collection should be limited to the data points that are necessary in relation to the purpose set forth.

Data should be processed in a legal and transparent manner.

Processing should be done in a way that ensures appropriate security of personal data and should not occur for a longer period than necessary.

All **collected data** should also be kept up to date and accurate at all times.



IMPORTANT NOTE

It is the responsibility of the controller to demonstrate compliance with these principles [Article 5(2)]. If you are an agency or consultant that is determining the data collection platforms and/or what to do with the data, following these principles is **your** responsibility.

The Basics

You must always have a valid and lawful basis in order to process personal data, which must be determined **before** processing.

Get it right the first time! You cannot change your legal basis without a very good, documented reason for doing so.

Also note that processing must be 'necessary'; the lawful basis will not apply if you can reasonably achieve the purpose by some other, less intrusive means.

Your Privacy Notice should specify your lawful basis along with the purpose for which the data is being processed

Six Lawful Basis Options

There are **six different lawful** basis options available for processing. No one basis is **"better"**, but the most appropriate basis will depend upon the **purpose and your relationship with the subject**.

Contract: To fulfill your contractual obligations to them or because they have asked you to do something before entering into a contract (providing a quote, for example).

Legal Obligation: You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.

Vital interests: Can rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life. However, if someone can give their consent (even if refused), then this is not a valid lawful basis.

Public Task: '*In the exercise of official authority*'. This covers public functions and powers that are set out in law or to perform a specific task in the public interest that is set out in law.

For Marketing and Advertising purposes, you will work with either: **Consent** or **Legitimate Interest**.

Consent: Processing after explicit and freely given acceptance by the user. The user must be transparently notified of the data collected, processing occurring, and how it affects them.

Legitimate Interest: Processing necessary for the purposes of your (or a third party partner's) business. These must be balanced against the rights and freedoms of the data subject's privacy and proven to outweigh the user's interests.

Consent

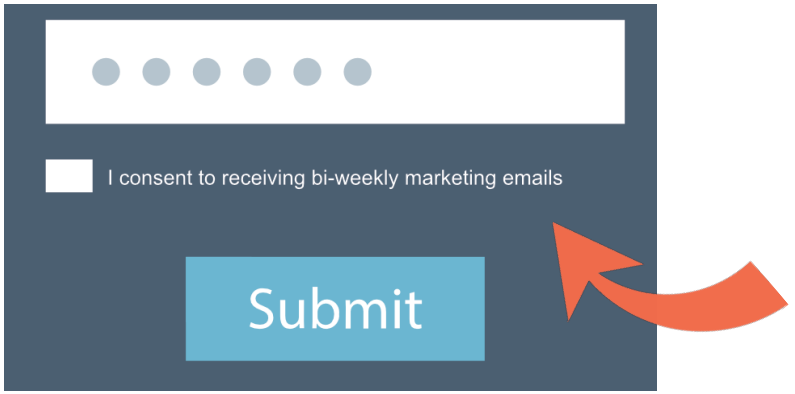
Consent is **difficult to obtain** but **easy to defend**!

Data Protection Directive (Current)

"Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"

GDPR

*"Any freely given, **specific**, **informed**, and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her"*



GDPR clarifies that the indication must be **unambiguous and provide a clear affirmative action**.

Consent Requirements Checklist

- [ ] Specific right to withdraw consent
- [ ] Clear and specific statements of consent
- [ ] Consent request messaging requirements
- [ ] No pre-ticked boxes and no “implied consent”
- [ ] Cannot be used as a prerequisite for a service
- [ ] Must be specific: Vague or blanket consent is not enough
- [ ] Consent must be separate from other Terms & Conditions
- [ ] All third party controllers relying on that consent must be named
- [ ] No set time limit for consent: This depends upon context, but it must be reasonable and defensible

Additional Consent Information

Consent Requests Should Include:

- *Name of organization*
- *Name of any third party controller relying on consent*
- *Why you want the specific data being collected*
- *What you will do with the data collected*
- *Notification that consent can be withdrawn at any time*

Always Maintain Evidence of Consent, Including:

- *Who consented?*
- *When did they consent?*
- *How was consent given?*
- *What was told to the subject/what did the subject give consent to?*

Recommendation:

Use a Privacy Portal. This allows users to manage their preferences across platforms and categories of data while also simplifying the documentation process.

LAWFUL BASIS FOR PROCESSING

Legitimate Interest

Legitimate Interest is **easy to obtain** but **difficult to defend**!

Requirements for Use

- Must show that use of personal data is proportionate, has minimal privacy impact, and people would not be surprised or likely to object to the use of their personal data in that particular way.

- Check also that it is compliant with Privacy Directives. For example, PECR (in the UK), requires consent for storage or access to information stored on a user's browser or device (cookies).
  - *These directives **mandate** consent and notification. Though, here, consent can be implied.*

You MUST include the details and logic you are using for Legitimate Interest as Lawful Processing within your Privacy Notification, being clear and transparent about what your interests are.

In the context of marketing, the right to object is **absolute**. You must stop processing as soon as someone objects.

Three Elements of Legitimate Interest

Purpose Test: Identify a legitimate interest

Necessity Test: Show process is necessary to achieve stated purpose

Balance Test: Balance the organization's interest against subject's interests, rights, and freedoms

Legitimate Interest Assessment

Perform the Purpose Test

- *Why do you want to process this data? What do you hope to achieve?*
- *Who benefits from the processing and how?*
- *Are there wider benefits to processing?*
- *How important are the benefits?*
- *What would the impact of not processing this data be?*
- *Would your use of the data be unethical or unlawful in any way?*

Apply the Necessity Test

- *Does processing actually further the stated interest?*
- *Is this a reasonable way to accomplish the interest?*
- *Is there a less intrusive way to accomplish the same result?*

LAWFUL BASIS FOR PROCESSING

Legitimate Interest Assessment

Do a Balancing Test

- *What is the nature of your relationship with the individual?*
- *Is any of the data sensitive or private?*
- *Would people expect their data to be used in this way?*
- *Are you happy to explain it to them?*
- *Would someone object or find it intrusive?*
- *What is the potential impact on the person?*
- *How big of an impact might this have on the person?*
- *Are you processing children's data?*
- *Are the individuals vulnerable in any way?*
- *Are there safeguards that could minimize the impact?*
- *Can you offer an opt-out?*

Apply the Tests.

Weigh the Options.

If you can reasonably and defensibly say that what the organization and the individual are getting out of the processing outweigh any potential concerns for the individuals' privacy, then you can use legitimate interest as the basis.

Above All:
Keep a record of this assessment for all cases.

Eye on the Future:

In 2019/2020, the new ePrivacy Directive may require explicit consent for the collection of cookie data. GDPR would still allow for Legitimate Interest, but would need to do so within these new directives.

Individuals Have the Right to...

Be Informed: You must be transparent about your use of personal data. This is typically done through a Privacy Notice.

Access: To their data and any supplemental information, which is typically also included in your Privacy Policy (what data is collected and how it is used).

Rectification: Have their information rectified if it is inaccurate or incomplete.

Erasure: Also known as *'The Right to be Forgotten'*, includes deletion or removal of data when there is no further reason for processing.

Restrict Processing: Ability to block or stop the processing of their personal information. In this case, you can continue to store the data but it may not be processed any further.

Individuals Have the Right to...

Data Portability: Must provide the subject their data in a structured, machine readable format. This applies to personal data provided to a controller, data obtained on a basis of consent or performance of a contract, or when processing is carried out via automated means

Object: To processing based upon legitimate interest, processing for direct marketing, and processing for purposes of scientific/historical research and statistics. You must inform subjects of this right at the point of first communication and provide a way for subjects to object online.

Know About Automated Decision Making and Profiling: Any automated individual decision-making resulting in a decision without human involvement. This includes the use of big data to learn something about an individual's preferences, predict behavior, and/or make decisions about them.

GDPR restricts you from making these automated decisions in cases where a **legal** or **similarly significant effect** on individuals can occur. The types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision.

In most marketing and advertising cases, the additional considerations for profiling would not apply since there is not a legal or similarly significant effect. That said, it must still:

- *Comply with GDPR priciples*
- *Identify and record your lawful basis for processing*
- *Have processes in place so people can exercise their rights*

An example of profiling would be pricing changes based upon a profile or changes to a contract or offer based upon a profile.

Real Life Example: Travel sites increasing pricing based upon cookie profile and search history.

An Overview

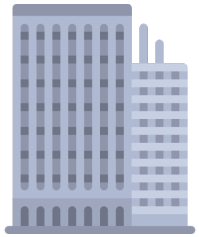
Article 5(2) summarized: *The controller is required to demonstrate compliance with the 6 Principles and that compliance is* ***your*** *responsibility.*

Organizational Measures

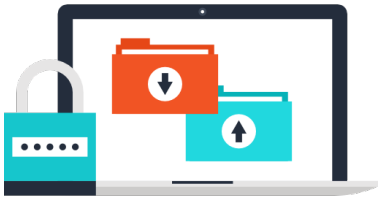
Privacy by Design and Data Protection by Default: Think through privacy for any new platform, data collection or marketing activity for what data is being collected, your lawful basis for processing, and if appropriate steps are being taken to protect the rights of the data subjects.

Documentation: Article 30

- *Privacy Notice*
- *Records of Consent*
- *Controller-Processor contracts*
- *Data Protection Impact Assessment Reports*
- *Records of Data Breaches*



Map the data flow or "Walk the Data": Understand where you're collecting personal data, what it's used for, where the data goes, who the processors and controllers involved are, and if you have the documentation in place to have a reasonable and defensible position for processing.



Technical Measures

- *Data minimization*
- *Pseudonymisation*
- *Transparency*
- *Allowing individuals to monitor processing*
- *Creating and updating security features on an ongoing basis*

AN OVERVIEW

Privacy Notice

You will want to cover each of the following areas when developing your privacy notice.

Basics:

- *Who are you? Include the Controller and the Data Protection Officer, if applicable.*
- *What you are going to do with a subject's information?*
- *Who will the information be shared with?*
- *In the case of legitimate interest: What is the reasoning?*

Determine Further Specifics:

- *Map information processing*
- *Items to work out (Implications of personal data that you are processing)*
- *These would all need to be reflected in the Notice*

Address the:

WHO, WHAT,

WHEN, WHY and

WHERE of personal data collection and processing.

If Sharing with Other Controllers:

- *Must identify who you are sharing with*
- *Need data sharing agreement in place with all controllers involved*

GDPR Requirements:

- *Concise, transparent, intelligible, and easily accessible*
- *Written in clear and plain language*
- *Free of charge*

For Analytics and Marketing

Analytics Data

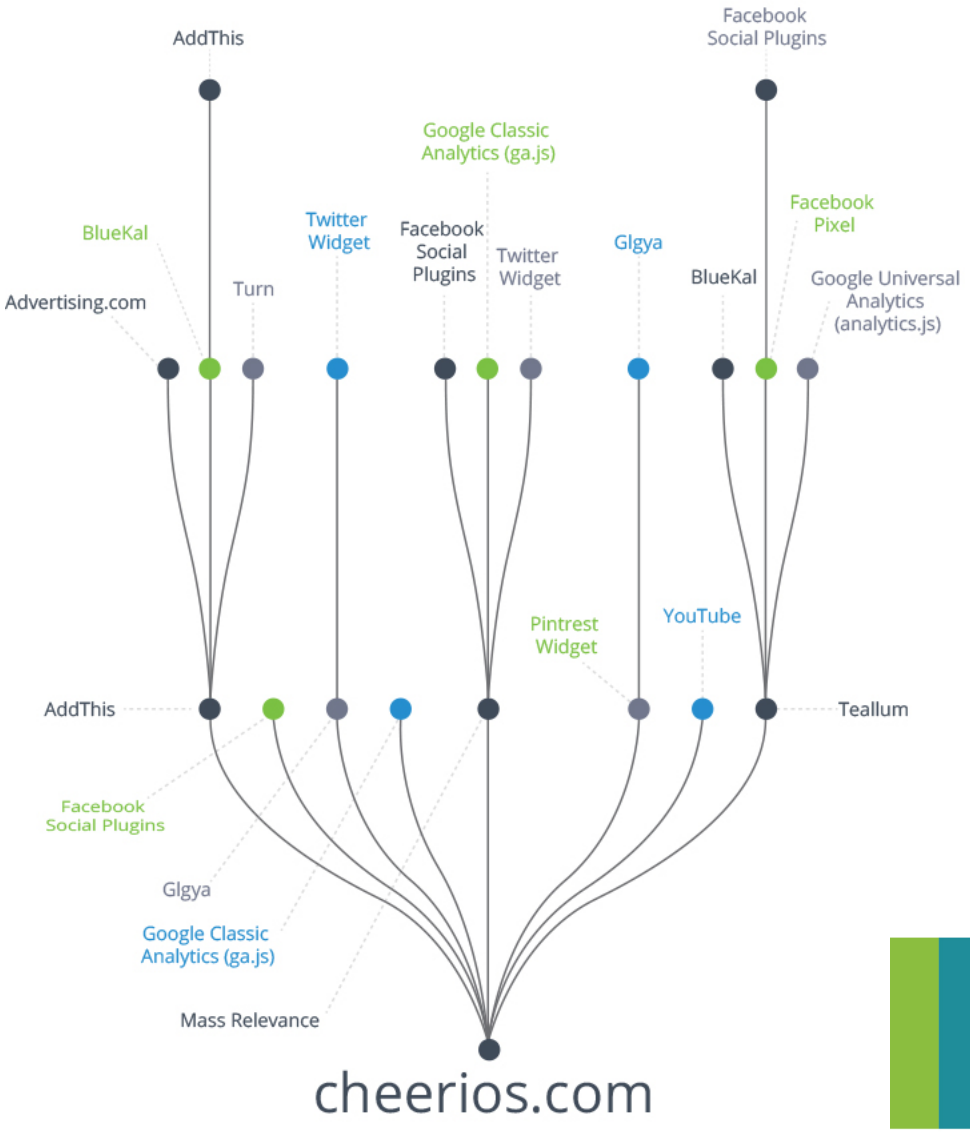
- Typically the only potential 'personal information' would be an anonymous cookie ID. Additionally, the information collected would be used in an aggregate format for statistical purposes.
- An analytics data set likely does not fall under 'personal data' in GDPR.
  - ***Careful!*** *As soon as you start combining this with additional data sets to provide context - such as location, IP address, email address - that would allow you to identify an actual person directly or indirectly using the cookie ID as the key, then the key and any data it collects becomes personal information.*
- Cookies are, however, covered in the ePrivacy Directives. So you must still be transparent about cookie usage and provide users the ability to opt out of analytics tracking.

Digital Media and Advertising

- Typically will be a much richer data set of personal and behavioral information than what you would have with analytics data.
- Therefore, the cookie IDs are likely to be treated as 'personal data'.
- Profiling will be taking place.
  - *If this profiling is not going to lead to adverse legal harm or similarly significant effects, the additional profiling permissions would likely not apply.*

WHAT IT ALL MEANS

Tag Audit



You must start with an understanding of **all the digital marketing** and **advertising** platforms currently on **your site**. A tag audit will allow you to see what tags are there and what data is being processed. From there, you can determine what data is being shared and with whom.

These are the foundations of compliance.

Review and Document

For Each Platform or Type of Data Collection

- Can it be classified as 'personal data' under GDPR? If so:
  - *What is the lawful basis for processing?*
  - *Are the Rights of the individual being adhered to?*
  - *Can you demonstrate adherence to the 6 Principles?*
  - *Is everything properly documented in the Privacy Notice?*

Moving Forward

- Build in a GDPR evaluation as part of purchase and on-boarding of any new marketing or analytics platforms
- Confirm all associated processors are GDPR compliant
  - ***Remember:*** *The onus is on the controller (that means you), so be sure that anyone you are sharing this data with is also compliant.*
- Ensure data sharing agreements are in place
- Maintain documentation!
- Monitor for new unvetted and unauthorized platforms

GETTING STARTED

With Tag Inspector

Tag Inspector is a tag auditing platform that is designed for marketers, by marketers.

If you manage a large site or multi-brand enterprise, **Tag Inspector's best-in-class tag library** and **real tag monitoring** in the **live environment** will give you unparalleled **data privacy, performance**, and **data quality peace of mind**.

ADDITIONAL RESOURCES

Learn More

- GDPR Text
- ICO UK Guidance
- ICO UK - 12 steps to take now (organizations)
- ICO UK Guidance - Privacy Notice
- ICO UK Guidance - Privacy Impact Assessments
- ICO UK Guidance - PECR
    - *Guidance for use of cookies*
- EU Article 29 Working Party Clarifications
- ICO GDPR Consent Guidance
- DPN Legitimate Interests Guide