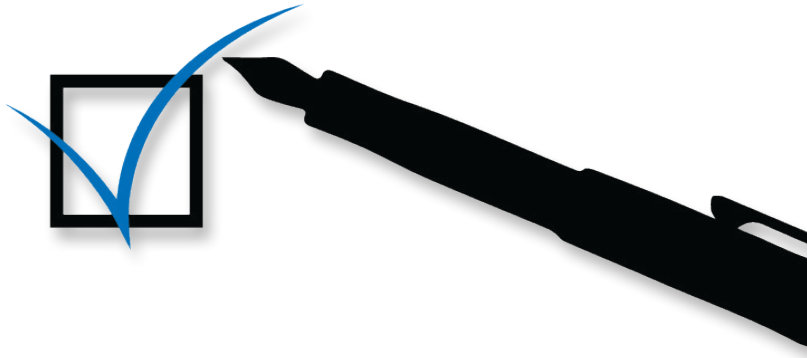
CONSENT



WHAT IS "CONSENT"?

Consent is one of the ways that you can allow your data to be used. In order to "consent" to your personal data being used, you should be aware of why your data is needed and how it will be used. Consent is essential to build the trust needed for the roll-out of new services. For example, you could be interested in one of your connected objects being able to play music when you order it to do so, but not to record your conversations permanently. On the other hand, giving your consent to process your musical taste so that you could be targeted with specific political advertising based on your perceived ideology might be less interesting for you (or for the future of democracy).

WHY IS THIS IMPORTANT?

The Eurobarometer 359 survey showed that 70% of Europeans are concerned about how companies use their data and feel they have only partial if any control; 74% want to be asked to give specific consent before their information are collected and processed. These findings were backed up in the latest topical Eurobarometer.

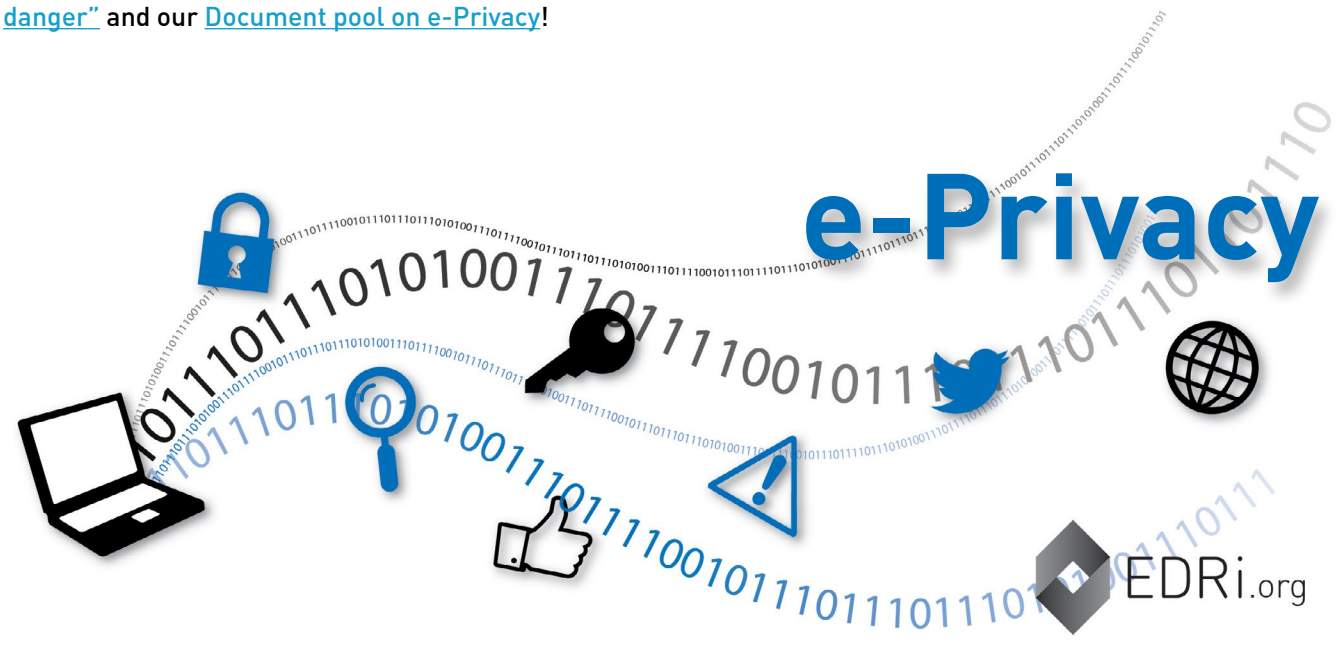
WHAT SHOULD THE E-PRIVACY SAY ABOUT IT?

Consent will drive the trust that is needed for new services. But consent also needs to be meaningful. It must be freely given, specific, informed and explicit, so that users can actually be in a position to give meaningful consent.

In order for consent to work, it needs to be as user-friendly as possible. The way that many apps are designed does not allow real consent. Accepting to all permissions required by an app that you want to use when the only alternative is not using it at all, is not consent. Moreover, even if the person in question could "consent" to one or other permission individually, it would be difficult for a general user to know how his or her information is being used by the software or any third party that has access to that information (such as an advertiser accessing a personal calendar, for example).

Communications data are highly sensitive. This is why every update of the e-Privacy Directive insisted on users' consent for processing of this data. Despite the claims to the contrary, the new Regulation is doing little more than maintaining this principle.

Do you want to know more? Check out our series of blogposts "Your privacy, security and freedom online are in danger" and our Document pool on e-Privacy!



LEGITIMATE INTEREST

WHAT IS "LEGITIMATE INTEREST"?

""Legitimate interest" is a legal basis for using **non-sensitive** personal data in certain circumstances, without consent.

Communications data (your emails, calls over the internet, chats...) must be treated as **sensitive** data, both logically and following the case law of the Court of Justice of the European Union. As the "legitimate interest" exception allows only the use of non-sentitive data, communication data cannot, logically and legally, be processed under this exception.

The "legitimate interest" exception (in the General Data Protection Regulation, GDPR) is generally used in circumstances such as incidental re-use of data by companies for the provision of services. This kind of circumstances do not arise with regard to sensitive communications data.

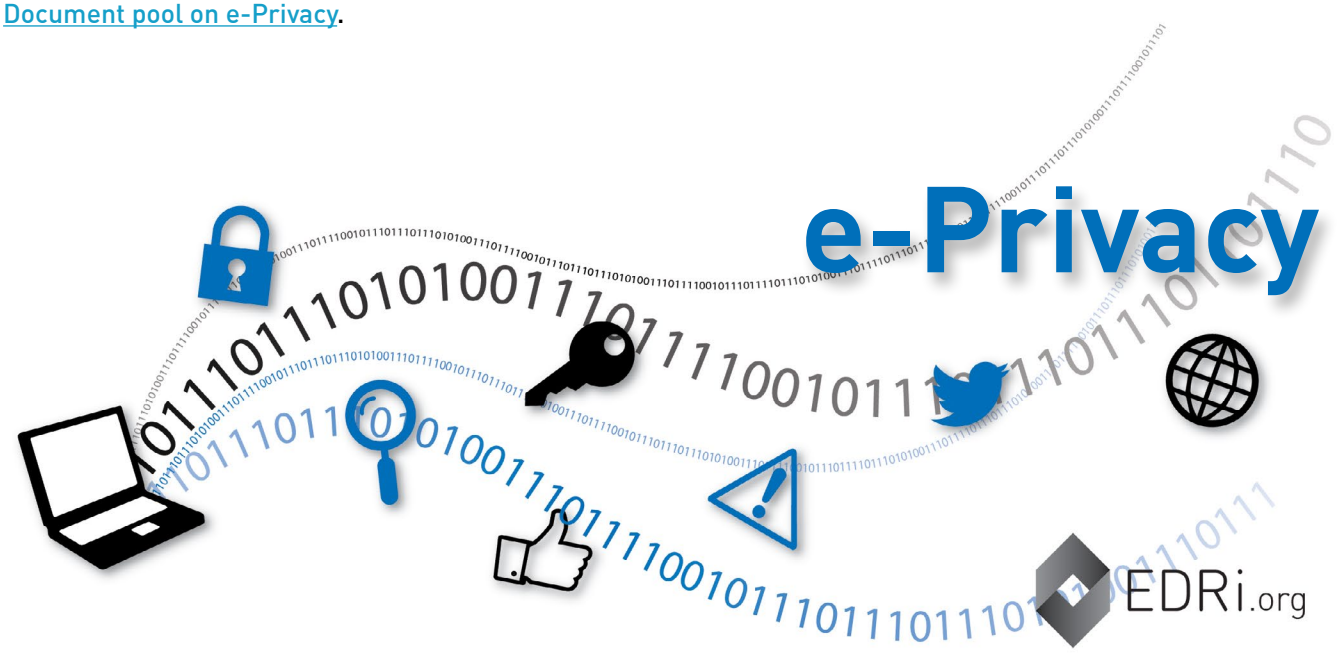
WHY IS THIS IMPORTANT?

Adding a "legitimate interest" exception in the e-Privacy Regulation would contradict the approach taken over the past 15 years in the European Union. It would contradict the the Tele2 ruling of Court of Justice, that ruled that communications data must be considered to be sensitive. Following the logic of that ruling to this ruling, companies should in no circumstances be allowed, without specific permission, to monetise or otherwise exploit sensitive communications.

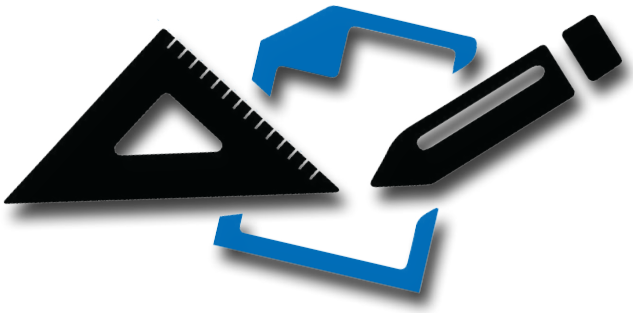
WHAT SHOULD THE E-PRIVACY SAY ABOUT IT?

Legitimate interest has no place in the e-Privacy Regulation. It would broaden to an unpredictable extent the way that companies (for example, direct marketers) would be allowed to use communications data. Any "legitimate interest" exception would undermine users' control over their own personal data, and would undermine their freedom of expression by creating the possibility for companies to analyse sensitive private communications without consent.

Do you want to know more? Check out the paper by EDRi member Bits of Freedom here. You can also find more about privacy in our series of blogposts on "Your privacy, security and freedom online are in danger" and our Document pool on e-Privacy.



PRIVACY BY DESIGN AND BY DEFAULT



WHAT ARE "PRIVACY BY DESIGN" AND "PRIVACY BY DEFAULT"?

Privacy by design is the principle by which all stages of creation of the hardware and software incorporates a high level of protection of your privacy. It is a principle that can be extrapolated from other circumstances in your life: lifts or cars do not have safety features added at the end, they are part of the design of the products. The same should happen with all the connected devices we use to communicate: smartphones, tablets, computers on so on. Similarly, privacy by default means that our devices and software are set to protect our data, with options to change this, if we wish.

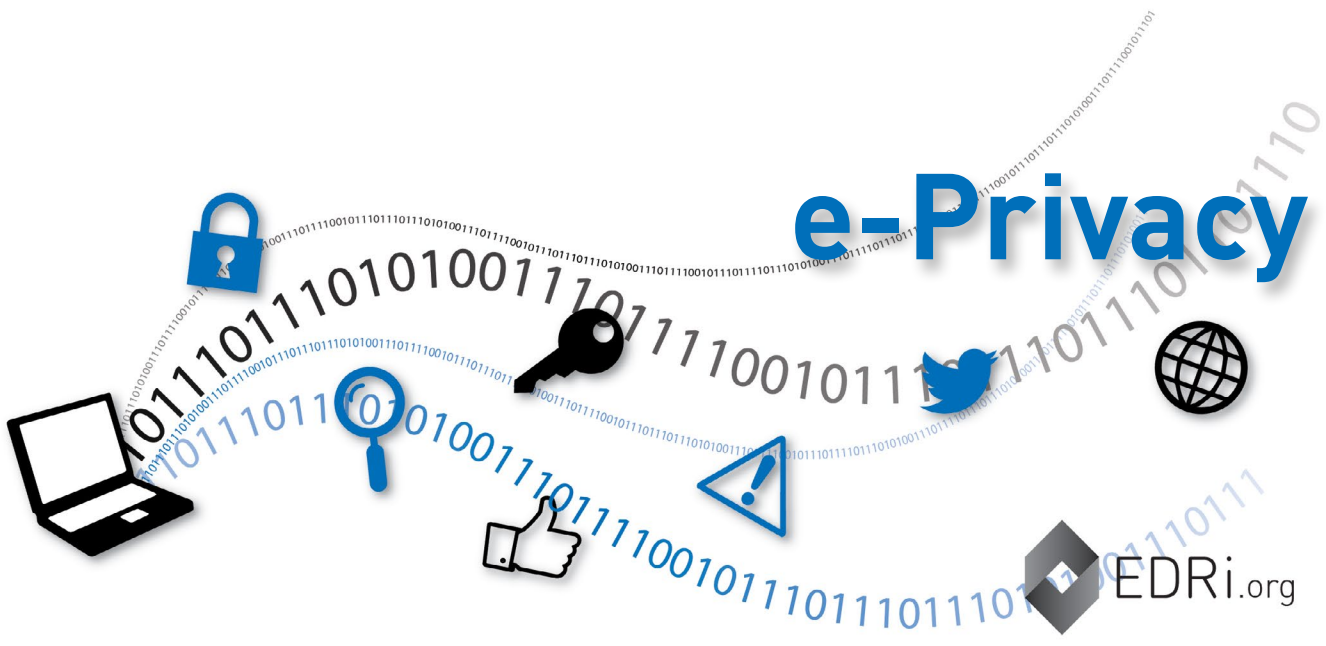
WHY IS THIS IMPORTANT?

We use more and more devices that collect and process very sensitive information: where we are, with whom we talk and when, the content of those conversations... This technology is making our lives easier, but it could be used to undermine our security and to restrict our freedoms, if used inappropriately. We need to be in control of our machines, not the other way around.

WHAT SHOULD THE E-PRIVACY SAY ABOUT IT?

The e-Privacy Regulation will be the main framework to protect your communications online. In the originally proposed text, instead of privacy by design and by default, the Commission proposed "privacy by option". If you have ever tried to change your privacy settings on any major online platform, you will know how well hidden these "options" can be. If this part of the proposal is not changed in the final Regulation, users will be less protected. Instead of "privacy by option", hardware and software (not only browsers) should be designed at all stages to protect the privacy of individuals **by default**.

Do you want to know more? Check out our series of blogposts "Your privacy, security and freedom online are in danger" and our Document pool on e-Privacy!



OFFLINE TRACKING

WHAT IS "OFFLINE TRACKING"?

Offline tracking is the way you can be tracked using other information than your online communications data. The location of your device (tablet, phone, pc) can be easily and accurately identified if it is connected to, for example, a public Wi-Fi or to a cell tower. Sometimes, this tracking is technologically impossible to evade: If you want to receive a call in your cell phone, your phone provider needs to find your phone in order to send you the call. In other situations, the location of your device as you move through a specific location (for example, a shopping mall) is used for different purposes (such as trying new ways to catch your attention, to analyse which shops are most visited...).

WHY IS THIS IMPORTANT?

This type of technology is highly intrusive. It is already widely in use and is not limited to busy shopping malls but is also used, for example, to map traffic flows on roads. The collected data not only reveals the behaviour of passers-by, but also includes individuals living in the neighbourhood. Moreover, in some contexts, such as in the vicinity of a religious establishment, a medical clinic or a sex shop, this information should be considered to be sensitive by default. The European Commission proposes permitting this type of tracking, provided there is some sort of notification to the individual. EDRi believes that the notification to the individual does not contribute to the essential protection of the rights and freedoms of the individual. Also, the Commission's proposal makes the incorrect assumption that there would be so few tracking networks that such an opt-out system could work in practice.

EDRi recognises that location services can provide benefits to society, for example traffic planning in cities based on measurements of traffic congestion and travel times between different points in the city during the day. However, obtaining this information through tracking of individual citizens poses severe privacy risks and possibilities for abuse (including the risk of mass surveillance by commercial or law enforcement entities).

WHAT SHOULD THE E-PRIVACY SAY ABOUT IT?

EDRi believes that the text around location privacy should be strengthened. The current e-Privacy Directive was drafted with concerns about the expansion of location based services, at the time based on proximity to GSM phone masts. The Directive treats location data as a separate category with more stringent rules, requiring clearer information on processing and extra opportunities for opting out.

In most cases, there are better solutions to obtaining location-based information than centralised tracking of individual citizens. Smartphone apps can obtain the device location (e.g. through GPS) without leaking it to a third party. Technical solutions based on local computation in the end-user's device should always be preferred over centralised tracking. The ePR should provide an incentive to develop technical solutions where citizens can provide location data to services without any privacy risks (privacy by design).

Do you want to know more? Check out our series of blogposts "Your privacy, security and freedom online are in danger" and our Document pool on e-Privacy!