We are pleased to present the *Moral-IT* and *Legal-IT* decks.

These physical cards are a responsible research and innovation tool created to enable structured reflection on legal, ethical, technical and social implications of new information technologies.

They are the latest development in our research at the Horizon Digital Economy Research Institute into the role of physical card-based tools in translating law and ethical principles into more accessible forms for design teams. Inspired by legislative changes, such as the new General Data Protection Regulation, we recognise the need to build *legal compliance* into technologies by design and default. High profile scandals of data misuse have increased calls for technologies to be developed in more *ethically* sound ways too. We feel that practical tools for actually doing this and bringing wider values into IT design are lacking. These cards seek to address this gap, by supporting engagement with legal and ethical concepts through a process of translation into a more accessible form.

Our Moral-IT deck poses a wide range of critical ethical questions designers need to ask of their new technology. These are thematically clustered around four themes (privacy, ethics, law and security) and below are some examples.

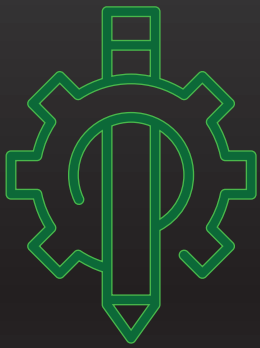
Our Legal-IT deck translates five complex European legal frameworks that aim to ensure data protection and cybersecurity for data driven technologies. We present the relevant rights, principles, definitions and responsibilities within the: **EU General Data Protection Regulation 2016; EU Draft e-Privacy Regulation 2017; EU Network and Information Security Directive 2016; Cybercrime Convention 2001; and Attacks Against Information Systems Directive 2013**.

The beauty of cards is they can be used in a wide variety of ways. One approach is as part of our streamlined impact assessment process to unpack risks, likelihood of occurrence, safeguards and challenges of implementation. This proves particularly useful for a team at the early stages of the design of a new application or technology. A board guiding you through this process is downloadable below. They can also be sorted by relevance, clustered thematically and ranked in terms of importance by designers. We have been testing these in a variety of contexts, most recently with research teams as part of the Horizon Services Campaign.

The cards are publicly available as downloadable PDFs which you can print off or send to a professional printer. We would really like to build up dialogue on **who** you are, **how** you are using the cards, **why** and any feedback you have on the tool/process. Please send these on to lachlan.urquhart@gmail.com.

Data Protection by Design and Default

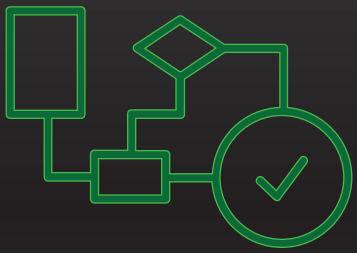
Art 25 GDPR



Technical & organisational safeguards should be built into processing by design & default to protect rights of data subjects & comply with the law. Costs, technical state of the art & degree of risk need to be reflected.

Profiling & Right to Algorithmic Explanation

Art 15 (h); 22 GDPR



Unless a decision is contractual or explicitly consented to, data subjects have the right not to be subject to automated decision making with legal effects e.g. algorithmic mortgage refusal. They can request human oversight & review of decisions made.

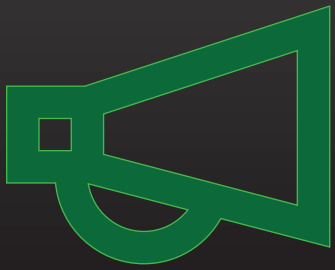
International Data Transfer Restrictions

Art 44 - 47 GDPR

Ordinarily, personal data should not travel outside the EU unless certain conditions are met, including: a bilateral agreement governs transfers; an EU adequacy decision exists; or model contract clauses are used.

Security Breach Notification to Users

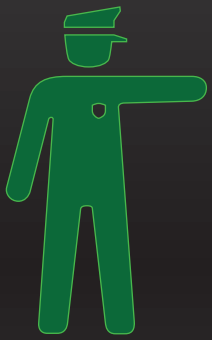
Art 34 GDPR



Controllers need to inform end users of a breach without undue delay if risks to fundamental rights and freedoms exist. They don't if the data is encrypted, mitigating measures have been taken or contacting all end users individually is too hard.

Security Breach Notification to Authorities

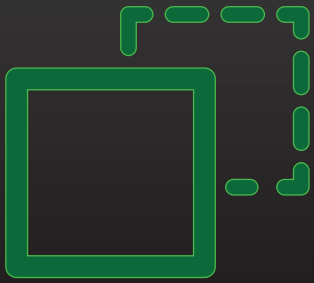
Art 33 GDPR



When a data breach may impact an end user's fundamental rights and freedoms, controllers should inform authorities, ordinarily within 72 hours depending on the nature, scale & consequences of the breach.

Greater Information Transparency

Art 12 GDPR



Information provided to end users must be concise, transparent, easy to understand & written in clear language.

Data Protection Impact Assessments

Art 35 GDPR

New technologies posing risks to fundamental rights and freedoms require systematic, docyumented analysis of risks, likelihood of occurrence, safeguards & implementation approaches.

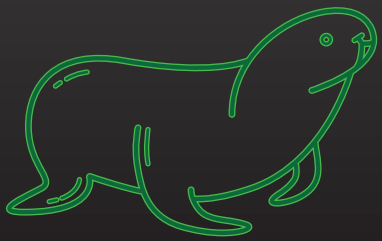
Responsiblities

Art 24 GDPR

Data controllers need to establish technical & organisational measures to ensure compliance with the GDPR, relative to likelihood & severity of risks to rights of data subjects.

Seals, Codes, Certification and Marks

Art 40-43 GDPR



Industry led GDPR codes of practice, certifications & seals are emerging for application domains such as on pseudonymisation or children's rights.

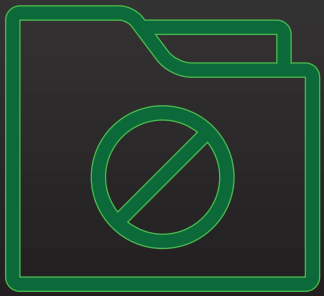
Right to Object

Art 21 GDPR

Users can object to their data being processed, particularly for direct marketing. After they do so, the direct marketer must stop using it.

Right to Restrict

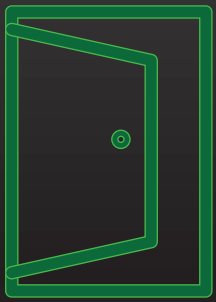
Art 18 GDPR



Users have a right to restrict data processing, instead of full deletion. Restricted data can only be processed in limited circumstances, namely with user consent or for the public interest.

Right to Access

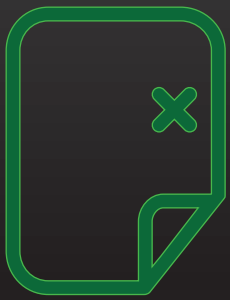
Art 15 GDPR



Users have a right to know who processes their data, why, where & what data is stored, how it is used & shared. They can request a copy for a fee.

Right to Rectify

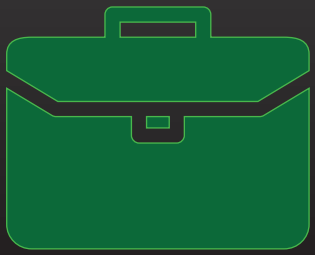
Art 16 GDPR



Users have a right to get inaccurate information corrected & incomplete data completed.

Right to Data Portability

Art 20 GDPR



Users have a right to request certain personal data in a structured, commonly used, interoperable & machine readable format e.g. CSV, JSON. They have a right to transmit this to another data controller.

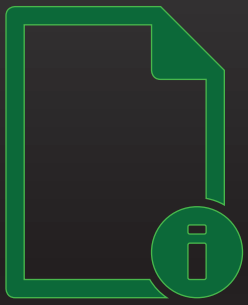
Right to Erasure/ 'to be Forgotten'

Art 17 GDPR

Users have a right to data deletion without delay. If user consent is withdrawn or data is no longer necessary, controllers must comply. Generally, this right is not absolute & must be balanced against freedom of expression or public interest.

Information on Rights Requests

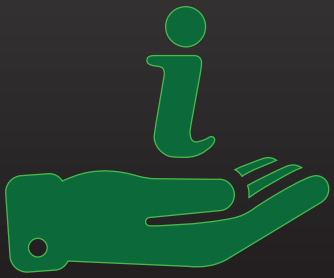
Art 13-14 GDPR



When subjects make requests under their data rights, information should be given within one month, exceptionally two. Ordinarily this is given electronically & free of charge.

Right to General Information

Art 13-14 GDPR



Controllers should provide users information on their identity, contact details, purposes and legal grounds of collection.

Special Categories of Personal Data

Art 9 GDPR

Political opinions, genetic & biometric data, health & sex life data, racial & ethnic origin, religious & philosophical beliefs, cannot be processed unless explicit consent is obtained or processing is necessary for certain purposes.

Data Supply Chain

Art 19 GDPR

Controllers should let all data recipients know about rectification, restriction or erasure requests too, unless this is too difficult or impossible.

Purpose Limitation

Art 5(1)(b) GDPR

Data can only be processed for defined purposes & cannot be used in ways inconsistent with these.

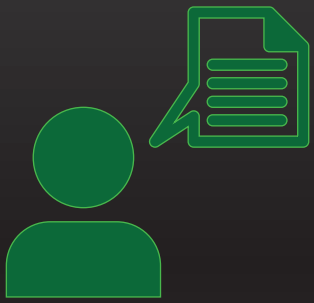
Lawful, Fair & Transparent Processing

Art 5(1)(a) & 6 GDPR

Lawful data processing requires data subject consent, or when necessary, other legal grounds can suffice i.e. in the public interest, controller's legitimate interests, to satisfy a contract or other legal obligation.

The Accountability Principle

Art 5(2) & 24 GDPR



Data should be processed in compliance with GDPR & this should be demonstrated to users & regulators through an account of actions taken.

Nature of Consent

Art 4(12) & 7 GDPR

Consent must be an unambiguous agreement to data processing that is freely given, specific & informed. Statements or other oral, written or electronic affirmations are needed.

Obtaining and Proving Consent

Art 7 GDPR

Consent must be provable, can be withdrawn at any time, & when given as part of a larger written contract, the details are flagged up in clear & plain language

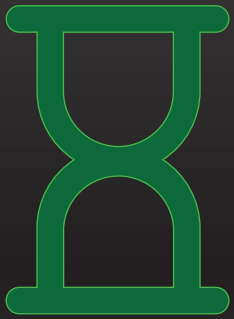
Children and Consent

Art 8 GDPR

Consent must be given or authorised by parents/guardians on behalf of under 16's when using online shopping, social media.

Storage Limitation

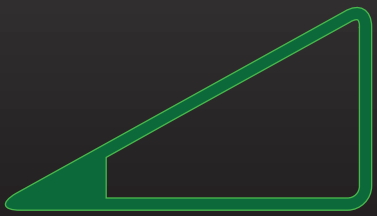
Art 5 (1)(e)



Data must only be stored as long as necessary for the purposes of processing.

Data Minimisation

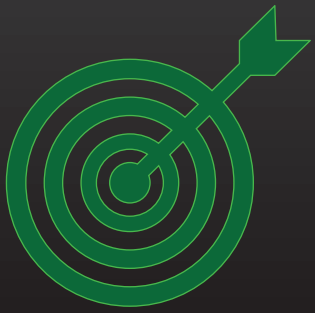
Art 5(1)(c)



Data collection must be limited & relevant, kept to the minimum necessary for the specific processing purposes.

Data Accuracy

Art 5(1)(d)



Data collection must be kept up to date & inaccuracies should be corrected or deleted quickly.

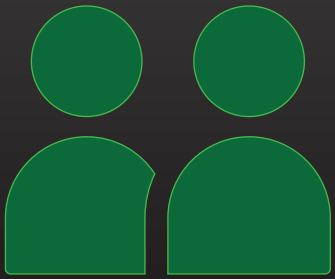
Restriction of Rights

Art 23 GDPR

Some data subject rights can be restricted by law in certain cases, i.e for national & public security; for prevention, investigation, detection & prosecution of crime.

Joint Controllers

Art 26 GDPR



Two or more data controllers may jointly decide the purposes & means of processing. Collective agreement of respective responsibilities & duties to subjects is needed.

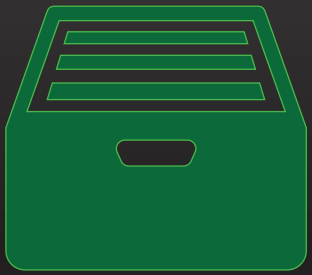
Controller, Processor & Outsourcing

Art 28 GDPR

A controller may define means & purposes of processing with a separate processor carrying this out. This relationship needs strict, contractual definition.

Record Keeping

Art 30 GDPR



Comprehensive records of processing need to be maintained by controllers and processors, including categories of data, recipients, international transfers & security.

Integrity and Confidentiality

Art 5(1)(f) GDPR

Data must be secured using technical and organisational measures to protect against unlawful loss, destruction, or damage.

Data Security

Art 32 GDPR

Technical & organisational safeguards proportionate to data security risks are necessary, particularly use of encryption, pseudonymisation, confidentiality, integrity & resilience testing.

Research Exemption

Art 89 GDPR

Data subject rights can be resitricted when data is processed for research purposes. Technical & organisational safeguards need to be used, particularly pseudonymiastion & data minimsation.

Sanctions

Art 84 GDPR

Fines up to 4% of annual global turnover or €20m can be charged for non-compliance with GDPR provisions including, data subject rights, consent & third country transfers.

Household Exemption

Art 2(2)(c) GDPR

GDPR does not apply to data processing by a natural person in the course of purely personal or household activities.

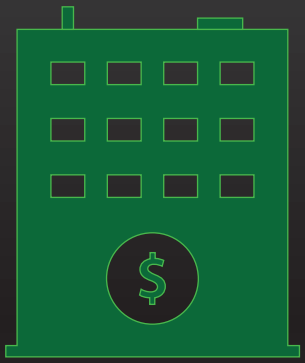
Personal Data?

Art 4(1) GDPR

Any information relating an identified or identifiable natural person. This includes direct or indirect identification, using identifiers (i.e. name, ID number, location data) or factors showing their identity (i.e. physical, mental, economic, social, cultural)

Data Controller?

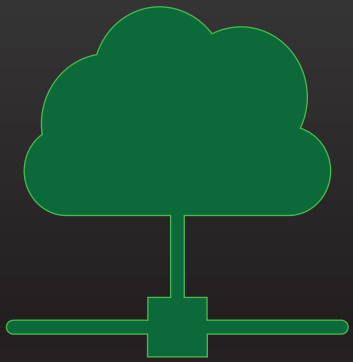
Art 4(7) GDPR



The entity that, alone or jointly, decides the purposes & means of processing i.e. social networking service, public authority, internet service provider.

Data Processor?

Art 4(8) GDPR



The entity processing personal data on behalf of the controller (i.e. contractually outsourced).

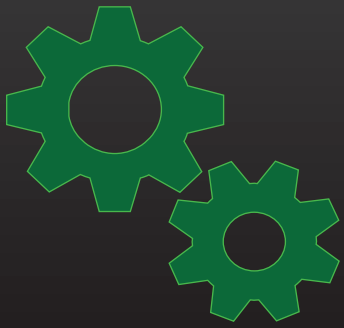
Data Subject?

Art 4(1) GDPR

The identified or identifiable natural person the personal data relates too.

Data Processing?

Art 4(2) GDPR



Processing is broad & includes any operations performed on personal data including use, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval...consultation.

Material Scope

Art 2 GDPR

GDPR covers data processed wholly or partly by automated means (computers). It also covers physical filing systems & information intended to form part of such physical systems.

Territorial Scope

Art 2 GDPR

GDPR applies to those offering goods or services & monitoring behaviour of EU citizens, even those outside Europe (i.e. US companies).

Personal Data Breach?

Art 4(12) GDPR

This is an accidental or unlawful breach causing destruction, loss, alteration, unauthorised disclosure, access to personal data.

Biometric Data

Art 4(14) GDPR

It is the outcome of a technical process related to a subject's physiological, physical or behavioural attributes. It enables unique identification of the subject i.e. fingerprints.

Health Data

Art 4(15) GDPR

It relates to physical or mental health of the subject and indicates their health status. It includes details of care provision.

Genetic Data?

Art 4(13) GDPR

It relates to an individual's unique inherited or acquired genetic characteristics. Based on a biological sample, this data indicates their health or physiology.

Pseudonymisation?

Art 4(5) GDPR

Pseudonymisation strips out attribution to data subjects, where reidentification requires additional information.

EU General Data Protection Regulation 2016

GDPR

?

Anonymisation?

Recital 26 GDPR

Truly anonymised data is not personal data and thus not covered by GDPR, but is technically difficult to achieve in practice.

The LegalIT Cards

Data Protection Law

DEFINITIONS

The LegalIT Cards

Data Protection Law

PRINCIPLES

The LegalIT Cards

Data Protection Law

RESPONSIBILITIES

The LegalIT Cards

Data Protection Law

RIGHTS

Cooperation

Art 9-13 NIS

Cooperation is essential for incident handling. This needs strategies, initiatives & awareness raising at national & international levels, including with CSIRTs.

Duty to Notify of Incidents (Digital Services)

Art 16 NIS

Notification to relevant authorities without undue delay is needed for substantial incidents. These are determined by duration & geographical spread of incidents; impacts to economic & societal activities, the extent of disruption & number of users affected. The public may be notified by authorities where necessary. Micro/small businesses are excluded from these requirements.

Incident Notification (Essential Service Operators)

Art 14 NIS

Notification to relevant authorities without undue delay is needed for significant incidents that affect service provision. These are judged by the number of users affected by disruption, incident duration & geographical spread of incident. This information may be shared with other member states to co-ordinate responses.

Network Security Requirements (Digital Services)

Art 16 NIS

Appropriate, proportionate technical & organisational measures to address risks posed to systems, relative to the state of the art, are needed. These need to ensure continuity of service & prevent/minimise impacts of incidents. They also need to provide security of systems and facilities; incident handling; business continuity management; monitoring, auditing & testing; compliance with international standards.

Network Security Requirements (Essential Service Operators)

Art 14 NIS

Appropriate, proportionate technical and organisational measures to address risks posed to systems, relative to the state of the art, are needed. They need measures to ensure continuity of service and prevent/ minimise impacts of incidents.

Computer Security Incident Response Teams (CSIRT)

Art 9/Annex I NIS

This national body is responsible for network and infosec risk & incident handling. Especially, for monitoring & responding to national incidents, providing early warning & situational awareness.

Voluntary Notification of Incidents

Art 20 NIS

Organisations that are not essential servies or digital service providers can nevertheless volunteer information on incidents that will impact continuity of their services.

Enforcement of Art 14 and Art 16 NIS

Art 15 & 17 NIS

With both Article 14 and 16 NIS, member states need to make sure that there are appropriate regulatory powers (including setting penalties) for authorities to enforce the rules.

Standardisation

Art 19 NIS

States should encourage use of European or internationally accepted standards on network & information security. EU body ENISA will help creating guidance & advice on this. They already have guides on smart energy grids & industrial IoT.

Essential Service Operators

Art 1/Annex II NIS

Private or public operators of essential, critical public infrastructure defined at country level, including providers of energy, transport, banking (credit institutions), finance (stock exchanges), health (hospitals), water supply or digital (Internet exchange point, domain name system, top level domain registries).

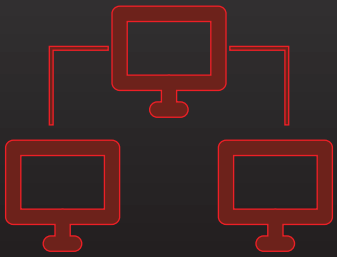
Network & Information System Security

Art 4(1) NIS

Ability of systems to resist action that compromises availability, authenticity, integrity or confidentiality of data or services reliant on the networks.

Network & Information Systems

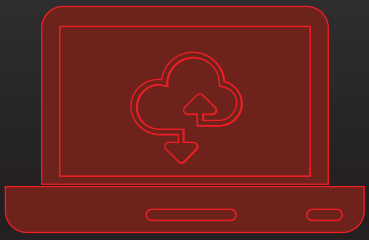
Art 4(1) NIS



The communications network plus devices programmatically performing automatic data processing (i.e. computers) plus data stored, processed retrieved or transmitted by the preceeding two.

Digital Services?

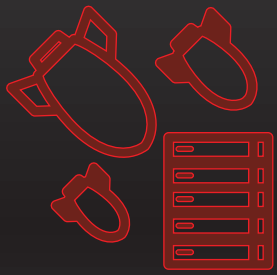
Art 1 /Annex III NIS



Online marketplaces, search engines & cloud computing services.

Illegal System Interference

Art 5 CCC / Art 4 AAIS



This criminal offence involves intentionally, seriously hindering the functioning of a computer/IS by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or making inaccessible computer data, without authority to do so.

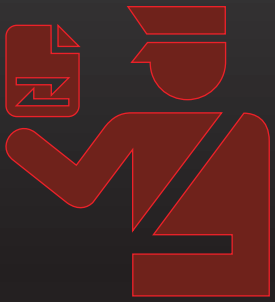
Illegal Data Interference

Art 4 CCC/Art 5 AAIS

It is a criminal offence to intentionally damage, delete, deteriorate, alter, suppress or make inaccessible computer data, without the authority to do so.

Illegal Interception

Art 3 CCC/Art 6 AAIS



It is a criminal offence to intentionally intercept non-public transmissions of data as they travel to or from a computer/IS, without authority to do so. This includes electromagnetic emissions (e.g. radio waves).

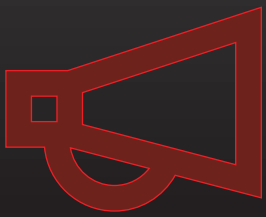
Illegal System Access/'Hacking'

Art 2 CCC/ Art 3 AAIS

It is a criminal offence to intentionally access a computer/IS without authority to do so. This could be done by infringing security measures with dishonest intent or in order to access computer data.

Illegal Interception

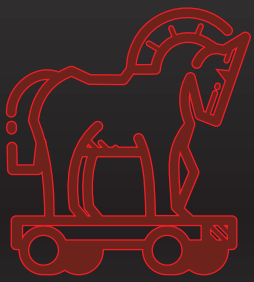
Art 3 CCC/Art 6 AAIS



It is a criminal offence to intentionally intercept non-public transmissions of data as they travel to or from a computer/IS, without authority to do so. This includes electromagnetic emissions (e.g. radio waves).

Misuse of Devices/ Creation of Hacking Tools

Art 6 CCC/Art 7 AAIS



It is a criminal offence to intentionally produce, sell, procure for use, import or otherwise make available tools (mainly computer programmes or passwords) with the intent they'll be used to commit the other offences. Possessing tools is also illegal, unless for authorised testing or system protection.

Computer Related Fraud

Art 8 CCC

It is a criminal offence to intentionally cause loss of property to another person by inputting, altering, deleting, suppressing computer data or interfering with functioning of a system, without authority & with fraudulent or dishonest intent to derive economic benefit.

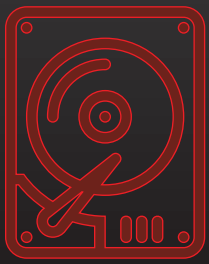
Incitement, Aiding, Abetting & Attempt

Art 11 CCC/ Art 8 AAIS

Incitement, aiding & abetting another to commit any of the access, interception, toolmaking or interference offences is itself a criminal offence. Attempting interference with a system or data, even if it fails, is also illegal.

Computer Data

Art 1(b) CCC/Art 2(b) AAIS



Any representation of facts, information or concepts in a form for processing in a computer system including computer programmes performing functions.

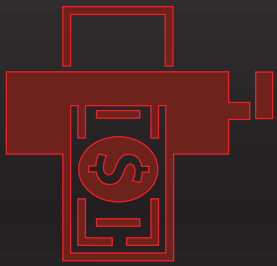
Computer/Information Systems (IS)

Art 1(a) CCC/Art 2 (a) AAIS

A computer system is device or group of interconnected/related devices that programmatically perform automatic data processing. An IS includes the device plus computer data stored, processed, retrieved or transmitted by devices for their operation, use, protection & maintenance.

Computer Related Forgery

Art 7 Cybercrime Convention



It is a criminal offence to intentionally input, alter, delete or suppress data to create inauthentic data with the intent it will be considered authentic. This stands even if data is not intelligible or directly readable. It could be done with fraudulent or dishonest intentions.

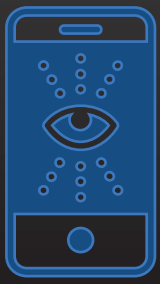
The LegalIT Cards

Cybersecurity & Cybercrime Law

RESPONSIBILITIES

Confidentiality of Communications Data

Art 5 ePrivacy; Recital 12



Both content & metadata shall be confidential incl. calls, internet access, instant messaging apps, e-mail. Data interference by anyone except end users is prohibited, unless the law permits it (see Art 6). This covers data 'listening, tapping, storing, monitoring, scanning, or other kinds of interception, surveilllance or processing' and applies to machine to machine communications too.

Processing of Communications Data (General)

Art 6 ePrivacy

Communications data can only be processed by relevant networks & services as long as necessary for successful communication transmission. When necessary for security reasons, it can be done for a limited time to either maintain or restore networks & services or detect faults & errors during transmission.

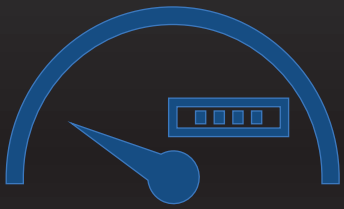
Processing of Communications Data (Content)

Art 6 ePrivacy

Consent is required for any use of content data. Content can only be processed for the specific service consented to & if there is no way to provide service without processing the content.

Processing of Communications Data (Metadata)

Art 6 ePrivacy



Metadata can be processed on three legal grounds: when necessary for quality of service e.g. latency; for business purposes like fraud prevention or billing; when consent is provided. Processing needs to be for purposes that could not be satisfied using anonymised data.

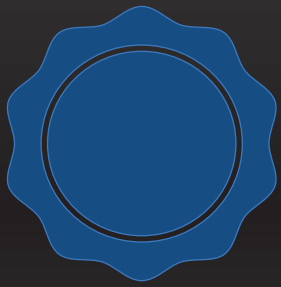
Storage & Erasure of Communications Data

Art 7 ePrivacy

Services need to anonymise or erase any communications data once it reaches the intended recipient(s). Content data can be stored by end users or third parties they trust, as per GDPR rules. Metadata can be kept for billing purposes up until the transactions can no longer be legally challenged.

Conditions for Collecting Information Emitted from Terminal Equipment

Art 8 (2) ePrivacy



Collection is only permitted when: 1) it is necessary & exclusively to establish a connection or 2) when a 'clear and prominent notice' is displayed detailing the responsible person, modalities & purposes of collection. Standardised icons & seals could also be used to communicate information. Technical & organisational safeguards, proportionate to security risk, are required too.

Prohibition on Collecting Information Emitted from Terminal Equipment

Art 8 (2) ePrivacy

Collecting any information emitted from terminal equipment trying to connect to another device or any network equipment is prohibited. This includes collecting MAC addresses; data to authenticate devices on routers for public or private WiFi; interfering with Bluetooth pairing.

Conditions for Information Collection & Using Processing/ Storage Capabilities of Terminal Equipment

Art 8 (1) ePrivacy

Access or use related to terminal equipment is only permitted when it is: 1) necessary & solely for a transmission over the network of communications; 2) based on consent 3) necessary for a requested information society service (ISS) e.g. social media site, online shopping service; 4) necessary for 'web audience measuring' by the ISS the user requested (e.g. website traffic monitoring).

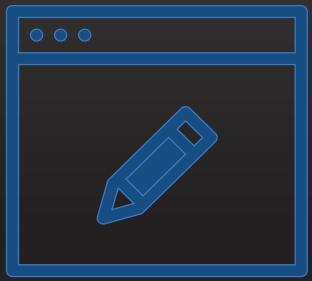
Prohibition on Information Collection & Using Processing/ Storage Capabilities of Terminal Equipment

Art 8 (1) ePrivacy

Unless the law permits, it is forbidden for anyone but the end user to use the processing & storage capabilities of terminal equipment. This covers collecting information from the user's equipment about hardware/software too.

Consent Mechanisms

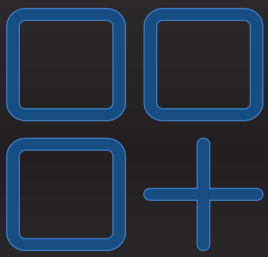
Art 9 ePrivacy



Consent is the same as in GDPR, i.e. any freely given, specific, informed, unambiguous indication of the data subject's wishes. It is a process, not a one-off act, withdrawable & should be rechecked every 6 months. Where possible, consent can be indicated by technical settings of the internet accessing software e.g. browsers.

Software Information Requirements & Communicating Privacy Settings

Art 10 ePrivacy



Where software enables electronic communications & retrieves /presents information from the internet (e.g. a mobile app), it needs options to prevent storage or access by third parties designed in. Privacy settings need to be communicated & consented to by users at installation, otherwise the software should not install.

Spam and Cold Calling

Chapter 3 ePrivacy

ePrivacy also provides rules on cold calling, call blocking & email spam, particularly on opting out.

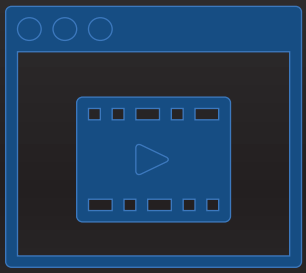
Terminal Equipment

Art 4(1)(c) ePrivacy

This is equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information...by wire, optical fibre or electromagnetically e.g. smartphones, laptops, tablets, PCs, gaming consoles, routers and IoT devices.

Electronic Communications Content

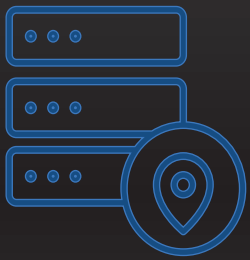
Art 4(3)(b) ePrivacy



'Text, voice, videos, images and sound' exchanged over electronic communications services. This could include web browsing behaviour, and possibly internet based TV viewing habits (e.g. Netflix).

Electronic Communications Metadata

Art 4(3)(c); Recital 14 ePrivacy



Data processed by the electronic communications network to transmit, distribute or exchange content i.e. traffic and location data including information on source/destination, location of a device, date, time, duration and type of communication.

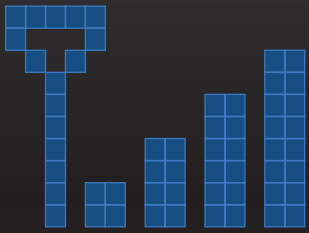
Electronic Communications Data

Art 4(3)(a) ePrivacy

It encapsulates both metadata & content data. It is distinct from the GDPR definition of personal data, although personal data may also be processed due to the services covered by ePrivacy e.g machine to machine, email, VoIP etc.

Relevant Networks

Art 4(1)(b) ePrivacy



It covers transmissions systems, permanent or temporary, centrally administered or not, using switching and routing for signals over wire, radio, optical or other electromagnetic means. This includes, satellite networks; fixed and mobile terrestrial networks (e.g. internet, mobile and landline telecoms); electricity cable communications; radio & TV broadcast; cable TV.

Relevant Services

Art 2(2) & 4(1)(b); Recital 13 ePrivacy

ePrivacy covers publicly available e-communications services with many over-the-top services like web based email (e.g. Gmail); instant messaging services (e.g. WhatsApp); VoIP (e.g. Skype); Group Chat & Messaging in games/social networking site/dating app (e.g. Tinder) & Machine to Machine (e.g. Internet of Things devices). It still covers telephony and internet access providers. It excludes services exercising editorial control (e.g. media services). It covers semi-private wifi hotspots within a city too.

Scope and Subject Matter

Art 1-3 ePrivacy

ePrivacy complements GDPR, providing more specialised rules in some circumstances.it is not constrained to personal data... It doesn't apply to law enforcement or national security bodies. ePrivacy applies to provision of e-communication services to EU citizens, even if no payment is given & protects information on EU users terminal equipment.

The LegalIT Cards

ePrivacy Law

RESPONSIBILITIES

The LegalIT Cards

ePrivacy Law

DEFINITIONS

The LegalIT Cards

ePrivacy Law

PRINCIPLES