EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on the protection of personal data processed through web services provided by EU institutions

November 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The web services of EU institutions ("web services") provide the user with a number of functions and services. In order to perform these functions and services the EU institutions may collect and process information related to the user or other individuals. More and more complex transactions are executed through these web services.

These guidelines are intended to provide practical advice and instruction to the EU institutions on the processing of personal information in the use of web services, to ensure that they comply with their data protection obligations as set out in the Data Protection Regulation No 45/2001 applicable to the EU institutions ("Regulation").

While these Guidelines are in principle aimed at the EU institutions (DPOs, DPCs IT services and web-services business owners), anyone or any organisation interested in data protection and web services might find them useful. The Data Protection Regulation applicable to the EU institutions, Regulation (EC) No 45/2001, is similar in many respects to the data protection Directive (EC) 95/46 and to the new General Data Protection Regulation (Regulation (EU) 2016/679), both of them applicable to EU Member States, as well as in the EEA. Other countries that look to the EU data protection model can find them useful, too.

The main topics covered in these Guidelines are:

- The use of cookies, scripts and any other tools to be stored or executed on the user terminal device.
- Server side processing of personal data and the wider issue of tracking.
- Main considerations in the use of third party services and personal data transfers.
- Web service specific security issues.

Summary of recommendations

These Guidelines focus on specific aspects of web services. These specific elements must be considered together with aspects applying to IT systems in general which are laid out in the "Guidelines on the protection of personal data in IT governance and IT management" in order to obtain comprehensive guidance on the protection of personal data in web services of the institutions.

First of all the institution should identify whether the web service processes personal data and what these data are. The Guidelines provide some guidance in this respect and the Data Protection Officer (DPO) should be asked for advice, too.

The ePrivacy Directive provides obligations to protect the confidentiality and integrity of communication terminal equipment. While formally binding for Member States, it applies in substance also to EU institutions. Consent for cookies and any analogue technologies requiring it (e.g. device fingerprinting) must be collected before setting cookies, after having adequately informed users about their utilisation. Specific conditions for a valid consent are described in the document. Consent should be the result of an active behaviour of the user indicating explicit acceptance. A sufficient level of granularity of choice must be provided. No "take it or leave it" approach is acceptable for public administrations such as the EU institutions, whose web services should be able to work also without cookies requiring consent. Their web services must provide mechanisms to manage consent according to these principles.

All records containing identifiers, including IP addresses, which can be used to single-out users, are considered as personal data and must be managed and protected as such. If the institution needs to track users, all the above considerations on consent management apply. If tracking is an intermediary step towards anonymous statistics, personal data must be anonymised as soon as possible and effectively. Though relevant testing is recommended, no re-identification attempts on real data should be performed. Pseudonymisation, even though a risk reduction measure, is not anonymisation and rules on personal data continue to apply.

Profiling is a practice bearing high risks to individuals' privacy. In this case, besides ensuring this is performed on a clear legal basis, the institution should perform a Data Protection Impact Assessment to better understand risks and provide strong safeguards.

Institutions must avoid using third party components that redirect users to web services they did not request and unlawfully transfer personal data, set cookies, track and profile.

If planning to use third party services, institutions must identify how the prospective involvement of the external organisation is to be considered under the Regulation (as "processor" or a new "controller" as a result of a "transfer"), and consider grounds for legitimacy and needed safeguards. If the conclusion is that these grounds do not exist or the institution cannot implement the needed safeguards, they must explore other solutions, including the choice of different external organisation/services or the opportunity of performing those tasks internally. Institutions should analyse whether the third party processes personal data for their own purposes and be sure that they take on board their responsibilities as "controllers" and adequately inform users. In this case, the institutions must verify the conditions for the transfer according to the Regulation.

Security is an essential component of personal data protection. The Guidelines recall some high level IT security considerations and introduce some web services specific issues. Institutions should manage information security risks jeopardizing personal data and identify needed security safeguards. Institutions should take into account known internet related threats and vulnerabilities, based on the specific web service architecture and technology. They should have documented procedures for web service secure development, deployment, operation and security testing following best practices, an integrated security testing approach and staff training policy. Managing vulnerabilities and an effective patching policy is essential for adequate protection. In case of particular risks for the web service or established breaches the institutions must, while considering possible high risks coming from disclosures, inform users and provide alternative communication means. The institutions must protect personal data sent over the Internet against risks to confidentiality, integrity and availability, including non-repudiation. Use of adequate cryptographic solutions for confidentiality of internet communications and authentication of the web service is highly recommended. Strict purpose limitation and retention rules exist for security logs, as well as strict necessity and proportionality must be ensured when processing data for security purposes. Personal data processed while managing data breaches need to be protected too by e.g. a progressive disclosure and a strict application of the "need to know" principle. The use of personal data in testing activities should be avoided or, when strictly necessary, adequately authorised and monitored. Anonymous browsing of institutions' web services should generally be allowed.

1. Introduction

1 For the purpose of this document, the term "web service"[1] includes any type of information service made accessible over the Internet with which users interact usually through web browsers or other client software technically called 'user agents". "Mobile" web services, which are designed to be better accessed by smart mobile devices via mobile browsers, are included.

2 Web services are a central part of the public interface of any organisation for the dissemination of information, collection of input and more and more complex transactions. Such role is clearly visible in the European Union institutions, bodies and agencies ("EU institutions"). As personal data is processed through these services, they must be operated in compliance with the data protection principles and with Regulation (EC) 45/2001 on the protection of personal data by Community institutions and bodies and on the free movement of such data[2] ("the Regulation"), so that the fundamental rights to privacy and to the protection of personal data must be guaranteed.

3 As the independent supervisory authority competent for the processing of personal data by the EU institutions, the EDPS may among other tasks issue guidelines on specific issues related to the processing of personal data[3]. The present guidelines are the result of a process where the EU institutions have been consulted.

4 These guidelines provide practical advice and instruction to the EU institutions as controllers on the application of the Regulation to development and operation of web services of the EU institutions. They are aimed at DPOs and DPCs within each EU institution, as well as IT and IT security staff, web services business owners and other administrative services concerned with the design or operation of web services.

5 While the purpose of the Guidelines is to make it easier for EU institutions to fulfil their obligations, they do not take away any of the responsibility of the EU institutions applying them. The measures recommended in these Guidelines are not intended to be exhaustive or exclusive. They are flexible enough to allow the EU institutions to start the expected process on accountability, and to be future oriented by considering expected legislative changes. EU institutions may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. Their effectiveness will need to be justified in writing.

---

[1] In the IT experts community the expression 'web service' often indicates a service over the internet for machine-to-machine interaction, usually in the context of a so called 'Service Oriented Architecture' where these services expose functionalities and interfaces that can be used by other services. Here the expression is used in a more general meaning and encompasses any services over the Internet.

[2] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[3] In the exercise of the powers conferred under Articles 41(2) and 46(d) of the Regulation.

2. Scope, methodology and structure of the guidelines

2.1. Scope and exclusions

6 This document focuses on data protection issues under the Regulation relating to the processing of personal data through the web services made available over the Internet by the institutions. This includes the protection of the confidentiality of communications as laid out in Article 7 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention of Human Rights (ECHR).

7 **The Guidelines address**, in particular:

- The use of cookies, scripts and any other tools to be stored or executed on the user terminal device.
- Server side processing of personal data including tracking.
- Main considerations in the use of third party components and services.
- Web service specific security issues.

8 They **do not consider/focus** on:

- Specific aspects of web applications for institutions' internal access.
- General data protection compliance requirements and accountability in IT governance and management[4].
- General IT security safeguards to protect personal data[5].
- Cloud computing architecture of EU web services[6].
- Monitoring of electronic communication activities for detection of unauthorised use of IT resources by staff of institutions[7].
- Protection of personal data for security and traffic management purposes (with the exclusion of what is specific to web services).
- The development and operation of mobile apps to interact with the institutions' online information resources[8].

[4]See forthcoming "Guidelines on the protection of personal data in IT governance and IT management of EU institutions"

[5]See "Guidance on Security Measures for Personal Data Processing Article 22 of Regulation 45/2001": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf

[6] The EDPS will issue guidance on the use of cloud computing services by European institutions and bodies

[7] See "Guidelines on personal data and electronic communications in the EU institutions": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-16_eCommunications_EN.pdf

[8] See "Guidelines on the protection of personal data processed by mobile applications provided by European institutions": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-11-07_Guidelines_Mobile_apps_EN.pdf

- Use of mobile devices by institutions' staff for professional purposes[9].

Some of these topics are dealt with in other EDPS thematic Guidelines.

9 **These Guidelines focus on specific aspects of web services. These specific elements must be considered together with more general ones applying to IT systems which are described in the "Guidelines on the protection of personal data in IT governance and IT management of EU institutions" in order to obtain comprehensive guidance on the protection of personal data in web services of the institutions.**

2.2. Methodology

10 The Guidelines contribute to action 8 of the EDPS Strategy 2015-2019[10], aiming to promote data protection culture, and accountability towards data protection requirements in the institutions through specific guidance. In particular, the EDPS has identified a need for specific guidance in protecting personal data when the processing operations are "technology intensive"[11].

11 These Guidelines are the result of a structured open dialogue with the EU institutions. The core steps/elements of this process are:

- A survey to start collecting facts and to understand the institutions' position.
- A workshop on the topic based on an orientation document sent in advance, where the EDPS also presented the survey results.
- A preliminary draft of the guidelines sent to EU institutions for their feedback.
- Taking into account such feedback, the finalisation of the guidelines.

12 These Guidelines will be revised by EDPS regularly re-engaging the EU institutions in an open dialogue process.

2.3. Structure

13 This document is structured as follows:

- Section 1 and 2 introduce the Guidelines and describe scope, methodology and structure.
- Section 3 examines when web services process personal data.

---

[9] See "Guidelines on the protection of personal data in mobile devices used by European institutions": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-17_Mobile_devices_EN.pdf

[10] See "EDPS Strategy 2015-2019 - Leading by Example": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-07-30_Strategy_2015_2019_Update_EN.pdf

[11] I.e. when the use of the technology characterises the processing operation in such a way that specific guidance on the use of that technology is needed to adequately protect personal data.

- Section 4 covers consent and information issues in the management of cookies and other client side techniques.
- Section 5 outlines the collection and processing of personal data on the server side, along with the wider issues of web tracking and profiling.
- Section 6 provides guidelines for processing personal data by third parties and in case of transfers.
- Section 7 covers web services specific security issues.
- Annex 1 contains a further legal analysis and guidance for the chapters

Text in italics and inside a box represents examples and clarifications to the content of the text above.

Rx: Recommendations come in boxes like this. Text with further advice and detail may precede or/and follow the box.

3. Personal data processed via a web service

R1: **The EU institution must assess whether a web service processes personal data and what**.

14 Personal data means any information relating to an identified or (directly or indirectly) identifiable natural person. In determining whether the information relates to an identifiable individual, the EU institution needs to take into account any means that could reasonably be used by them or any third party to enable the identification of an individual[12]. The institution should take into account the guidance given below and ask the DPO for advice.

R2: The EU institution must integrate the categories of personal data processed, as identified, in the notification to the DPO, as stated in Article 25 of the Regulation.

WHAT - Three categories of personal data can be identified:

- Those the web service processes for the business purpose it is designed for.

For example, the web service collects CVs to match employers' with jobseekers' needs, or contact details to send newsletters or publications.

- Those to enable users to log into the web service for authentication and customisation purposes.

- *Web service visitors might need to log in to use parts of the web service that are specifically crafted to them, according to their roles and needs.*

- Those the web service processes for other reasons (e.g. security, statistics) in addition to its main business purpose.

- *IP addresses[13], user identifiers, timestamps, URLs of the visited pages and other parameters are processed to create security logs or to build statistics on the usage of the websites.*
- *Further to that, if users are not logged in, other data could be collected to single them out via unique identifiers linked to their client terminal, such as IP addresses alone or jointly with other client side parameters or, for example, via their location data or cookie /terminal/ customer identifiers. See also Chapters 4 on cookies and 5 on tracking and profiling.*

15 HOW - Ways web services can collect personal data include these use cases:

[12] See also recital 26 of Directive 95/46/EC stating: "*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*"; similar recital 26 of the General Data Protection Regulation (see footnote 42): "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.* ".

[13] For the rationale on the need for IP addresses to be managed as personal data, see Annex 1.

- Web service users provide their personal information by e.g. filling in an online form (for receiving newsletters, submitting a petition, applying for a traineeship, organising a visit, lodging a complaint, etc.)
- The web service uses technology (e.g. so called "B2B gateways") to collect personal data from other internet sources.
- The web service uses cookies and similar technologies[14] in order to store and collect information already stored in the terminal equipment of the user.
- Functional and technical logs or network devices collect personal data of the web service users e.g. for statistics or security[15] purposes.

16 Note that personal data under the controller's responsibility are not only those originally collected via the web service, but also:

- Any other information that the controller has collected through other means and that can be linked to personal data collected through the web service.

For example, complaints sent as letters before a particular web service was set up to that end.

- Any other information inferred that relates to an individual.

It is possible to infer the identity of the individual or to relate some information to an already identified individual in a probabilistic way. Example: the use of device fingerprinting can lead to a certain percentage of assurance that two different sets of data collected belong to the same individual. Or, profiling individuals as belonging to certain behavioural categories based on data collected might include probabilistic matches and subjective decisions.

17 The EU institution is fully responsible for all processing of personal data caused by any interactions with the user agent that is performed by the web service, and must ensure compliance with the Regulation. This includes when third party services are used as processors or when third party services act as separate controllers.

[14] See chapter 4 of the Guidelines
[15] See section 7.2.6.1 of the Guidelines

4. Consent and information to users for cookies and other client side techniques

4.1. Introduction

18 It is of the utmost importance that web services users are in control of their data. Complete, clear information and an unambiguous, specific expression of users' will are key factors for users to be in control.

19 This chapter presents the obligations and recommendations that controllers should follow in relation to the consent and information to users when using cookies and similar technologies in their web services, in the light of Regulation 45/2001 and Article 5(3) of the ePrivacy Directive[16].

20 Firstly we introduce the relevant technologies covered by this chapter. Then we give guidance on when consent is required, how to obtain and manage valid consent for cookies and similar technologies, including what information to communicate to users.

4.2. Technologies under scope

21 The technologies covered by the considerations made in this chapter include:

- Cookies[17].
- Scripts (such e.g. JavaScript code) and components (such as browsers plug-ins[18]) to be executed on the client side.
- Web caching mechanisms[19].
- HTML5[20] local storage (see further on).
- "Device fingerprinting"[21] (see further on).
- "Canvas fingerprinting" and "Evercookies" [22]
- Web beacons[23]

---

[16] Directive 2002/58/EC as amended by Directive 2009/136/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF

[17] HTTP cookies : http://tools.ietf.org/html/rfc6265

[18] E.g. Adobe Flash - hence the name of Flash cookies - through the Local Shared Objects technology, or Microsoft Silverlight, through the Silverlight Isolated Storage technology.

[19] ETag is an HTTP protocol header field (see http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html) mainly used to validate web caches and allow more efficient browsing. It has also been used for cookie-like purposes.

[20] http://www.w3.org/TR/html5/

[21] RFC6973 defines fingerprinting as "the process of an observer or attacker uniquely identifying (with a sufficiently high probability) a device or application instance based on multiple information elements communicated to the observer or attacker". See http://tools.ietf.org/html/rfc6973

[22] Recently discovered advanced tracking mechanisms, hard to detect and neutralise. See e.g. https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

[23] See e.g. https://en.wikipedia.org/wiki/Web_beacon. Web beacons (often also called "web bugs") are invisible elements set on a web page to redirect the user client to a third party web service for tracking purposes in a hidden way. These can even take the form of a single transparent pixel.

- Any other technologies insofar as they enable reading or storing information from/onto the web service user's client device[24].

22 Cookies: Strictly defined they are pieces of text generated by the web services that the user has visited. Web services store these text files on the devices where the web browsers are installed to enable the exchange of information with their own web service or with others using those cookies. They were originally conceived to make up for the web protocols inability to record preferences (e.g. languages) or actions already performed on website (such as the articles already in the shopping basket of an e-commerce website). Later on their use was extended to enabling user authentication during a session, recording browsing behaviour[25] for web service improvement purposes, or for tracking and profiling users, e.g. to serve targeted advertising. Some main related concepts:

- Cookie lifespan: defined by the web service setting them, it can range from the duration of the current user session to longer periods (several years).
- First party and third party cookies: cookies are linked to a web domain and can only be sent back to the domain they are linked to. Often though, when requesting a web page, this page also contains elements from other web services, like advertising partners, social networking sites or other content providers. As a result, both first party cookies set by the site the user requested and third party cookies can be set on users' devices.

23 HTML5 is the latest standard web service language and automatically enables a cookie-like behaviour called HTML5 local storage. The information kept in the HTML5 local storage has no expiration and needs to be actively deleted. HTML5 has a far larger storage size than cookies and no plug-ins are needed. It represents a technology with many advantages, but has also data protection risks.

24 Device fingerprinting[26] is a technique used to collect sets of web user agents' parameters transmitted by the web protocols to the web services when interacting with them. It is used for purposes similar to those of cookies (e.g. user agent interface optimization, analytics for web service improvement and marketing, profiling for targeted advertising).

25 Device fingerprinting and other techniques other than cookies are reportedly often being used in an attempt to circumvent the ePrivacy Directive. The WP29 has clarified the issue by tackling this challenge in one of their Opinions and clarifying when and how the ePrivacy Directive applies[27].

---

[24] Thus falling within the scope of Article 5(3) of the ePrivacy Directive
[25] Commonly known as "analytics".
[26] See e.g. https://lirias.kuleuven.be/bitstream/123456789/393661/1/ for an overview on device fingerprinting
[27] See WP29 Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

As a result, in the context of these Guidelines, when we use the term "cookie" we also address each and every one of the tools mentioned above.

4.3. Obligations, recommendations and best practices

26 Whenever some information is accessed or stored on a user's device, the user must be given adequate information on what is accessed or stored and on the purposes of this action and means for expressing their consent must be given. No action may be performed before the consent is collected. Users must be enabled to withdraw their consent at any time.

Consent should be unambiguous and specific. It must also be "freely given", so the EU institution must not face users with a "take it or leave it" approach (often called "cookie wall")

Consent is not required by the law when cookies are used to enable the communication on the web and when they are strictly necessary for the service requested by the user. Nevertheless, even in these cases it is still necessary to provide the required information.

A cookie may only be considered strictly necessary if the service as such would not function without it. The choice of a certain implementation technique that relies on cookies is not sufficient to justify strict necessity if the EUI has the choice of a different implementation that would work without cookies.

For more detail on the legal requirements, see Annex 1.

4.3.1. Cookies requiring consent

R3: The EU institution must adequately inform users and obtain their consent before setting cookies and any other technology falling within the scope of Article 5(3) of the ePrivacy Directive. By default, none of those cookies must be set.

27 Cookies that **generally DO need consent**:

- Social plug-in tracking mechanisms.
- Third party advertising cookies.
- Analytics cookies (except for the exemption described further on in this section).

28 Cookies that **generally do NOT need consent**:

- User input cookies, for the duration of a session
- Authentication cookies, for the duration of a session
- User centric security cookies, used to detect authentication abuses and linked to the functionality explicitly requested by the user, for a limited persistent duration
- Multimedia content player session cookies, such as flash player cookies, for the duration of a session
- Load balancing session cookies, for the duration of session.

- User interface customisation cookies, for a browser session or a few hours, unless additional information in a prominent location is provided (e.g. "uses cookies" written next to the customisation feature)

29 Exceptionally, Data Protection Authorities consider that, due to the low risk for users, prior consent can be skipped in case of **first party cookies used for anonymous, aggregate statistics under specific assumptions and safeguards**[28]:

- The purpose of those statistics shall be only the measurement of the way the website is used for the improvement of its features and for purposes strictly related to the institution policies the website supports.
- Personal data shall not be used for purposes other than the specific statistics they were collected for.
- No tracking of users across websites managed by different owners is performed.
- The web service must provide the user with a simple, easy-to-use functionality to "opt out" from analytics, to be referenced in a prominent place of any landing pages of the web service itself.
- A strictly limited retention time for unique identifiers, such as IP addresses, shall be set, based on necessity and proportionality. Since in general one year is the longest coverage for statistics on unique user behaviour, the identifiers originally collected shall be deleted after about 13 months.
- Parts of the IP address shall be masked to mitigate the risk of users' identifiability that could arise e.g. from the possible link between the IP address and other natural identifiers, including the location of the user.

For example, if the IP address is used to determine from where the user accesses the website, then some parts of the IP address that are not necessary to that purpose should be masked depending on the necessary precision of the location.

4.3.2. Information to web service users and ensuring data subject's rights

R4: The EU institution must provide **adequate information on the cookies they use**.

R5: If cookies are used to collect personal data, the EU institution must also provide data subjects with all information under Article 12 of the Regulation. See "Guidelines on the protection of personal data in IT management and IT governance of EU institutions".

R6: A **layered approach**, where the information is given at different stages providing greater detail, should be used. Nevertheless, the essential information[29] should be present at a sufficient level of detail to put the user in control already at the first layer.

[28] See Annex 1 for a detailed background.
[29] See "Guidelines on the protection of personal data in IT governance and IT management"

R7: A notice providing (the reference to) the **first level of information on cookies** must be **clearly visible** to web service users **whatever their landing page**

30 In particular, the EU institution should provide at least the detail on the first level:

<u>First level info</u>

- Whether the cookie is first party or third party one.
- In case of third party[30] cookies:
    i. Identity of the third party.
    ii. Information given to data subjects by the third party (the same as required from the controller) or reference to the third party's webpage(s) containing that information. If the third party information is incomplete, the controller takes on the responsibility to complement it.
    iii. Link to third party data protection notices.
- Cookie purpose: sole transmission of info; strictly necessary for the service requested by the user – and details on how they serve this purpose; storing user preferences; social plug-in content sharing cookies; social plug-in tracking cookies; third party advertising cookies; first party analytics; third party analytics; other possible categories.
- Type of data collected and then stored and transmitted by cookies.
- Time limit for the cookie/data retention.
- How to give and modify consent to cookies (if required).

<u>Further levels info (optional but recommended):</u>

- Cookie names and typical values should also be present.
- Information on further ways for the user to be more in control, e.g. reference to frequently used user agents' data protection features, is envisaged.

31 When providing this information, using an external reference that is not under the institution's responsibility implies several risks, including also possible policy choices that could differ from those of the Regulation and of these Guidelines and be in breach of applicable law. As a consequence:

[30] The EU institution is responsible for all interactions with the third party service that happens when the user uses the EU institution's web service. This can happen when the third party service is a processor or a separate controller. See also section 3.

R8: We strongly recommended that the EU institution provide information on cookies **on the web service under their control and not rely on external sources**. If for some reasons the institution uses external sources, they should set up measures to manage relevant risks, where possible.

32 If an external source is referenced (e.g. the website of another DPA) the cookie notice should clearly explain what part of that source is to be relied upon (e.g. only some specific technical advice) and integrate a disclaimer on relevant responsibilities.

Nevertheless, the use of resources under the institution's control remains the best option.

4.3.3. How to obtain and manage valid consent for cookies and similar technologies

33 Consent needs to be collected in a way that ensures its validity. This implies that:

R9: The EU institution must give the users simple **tools to easily express and manage** (e.g. withdraw) **their consent** at any moment and for each and every category of cookies, depending on their purpose and origin (first or third party).

For example, if a website features cookies for user interface customization, for two different analytics services and for two different video steaming platforms, the tool must enable the user to express and withdraw consent for each and every of these purposes, and in particular for each and every of the analytics and video streaming services.

R10: The EU institution should **recommend that users read the cookie notice** and collect consent in the section of the web service where clear and comprehensive information on cookies is given.

R11: The EU institution must collect consent as the result of a user's **active behaviour** that leaves no room for interpretation of the user's choice. As a result, an **explicit consent** to the way cookies are used in the web service is considered as **the most appropriate way of expressing consent**. Continuing using the web service does not guarantee unambiguous consent.

34 The mechanisms implemented in current browsers are in general not adequate[31] to express explicit consent through specific settings[32]. The institution should therefore seek confirmation through other technical and organisational means (forms, banners etc.). See section 5.3.4 when such settings express the user's will **not** to be tracked.

[31] See e.g.; WP29's letters on DNT draft standards of 06/06/2014 and 01/10/2015. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm. See also footnote 32.

[32] See Recital 66 of Directive 2009/136/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF. These mechanisms include the W3C Tracking Preference Expression draft standards - also called Do Not Track (DNT) - as defined at the stage of drafting these guidelines. See: http://www.w3.org/2011/tracking-protection/.

35 EU institutions play a unique public role and provide public services through their web services. In this capacity:

R12: The EU institution should **design their web services** and **choose features and services** so that **none of the cookies that need prior and informed consent are necessary** for that web service to provide the essential institutional services.

For example, if the user does not accept third party cookies coming from social networking web services, such as video sharing services, this should not prevent them from using the essential services of the institution's web service, for instance, the submission of a complaint. The EU institution should explore alternative services or means to share those videos.

R13: The consent management mechanism provided by the EU institution should enable the institution to **demonstrate** that **consent was obtained** and how.

36 Collecting consent is not required for each and every use of the web service but its validity along the time should be appropriate with respect to the type of the services and the frequency of use.

R14: The EU institution should **periodically remind the user** that they gave their consent and of what they consented to. The frequency of reminders may depend on the frequency of use. Daily users should receive reminders less often. Users that have not used the service for several months may be reminded every time.

4.3.4. Cookie (and tracking) "respawning"

37 This technique is used for tracking when it is not possible to link new and old cookies because the old ones were deleted by the user or somehow disappeared from the client side. Respawning consists in using another technology (e.g. Flash cookies or web caching options or HTML5 storage or device fingerprinting) that enables bridging the old and the new identifier, thus creating a unique tracking pattern.

R15: The EU institution should not use **cookie "respawning"** if the processing relies on users' consent.

38 If cookies requiring consent have disappeared, this is most probably because the user deleted them and wanted to withdraw consent. Cookie respawning would circumvent the user's will. In this case the EU institution must collect again user's consent.

39 If, for any lawful purpose not based on consent, cookie respawning proves "strictly necessary", then transparency, proportionality, security and further safeguards need to be taken into account when choosing and implementing the respawning technology.

4.4. Further legal analysis and guidance

40 Annex 1 analyses the applicability of Regulation 45/2001 for processing personal data through cookies and similar technologies and the substantial applicability of Article 5(3) of the ePrivacy Directive, the need for consent and conditions of valid consent.

5. Server side processing, tracking and profiling

5.1. Introduction

41 This chapter focuses on processing operations involving the tracking and profiling of individuals that interact with institutions' web services. It highlights relevant data protection risks, and proposes guidance to manage those risks and comply with the Regulation and any other applicable provisions. A more detailed introduction on these topics is provided below.

5.2. Technical environment and risks

5.2.1. Web protocols, logs and data protection

42 Several log types are used to support web services. Logs can be generated by network devices like firewalls, proxies and intrusion prevention and detection systems, web and application servers and web applications for technical verification, functional and compliance auditing and security purposes.

43 Internet protocols enable the transmission of information from the client to the server side. They have been designed mainly for transmitting in a reliable way the required pieces of information from the origin to the destination, ensuring integrity, timely delivery and, for some of them, a degree of security.

44 Data protection principles like data minimisation with respect to the protocol usage purpose, and higher level of security to counter a growing level of surveillance and hacking expertise linked to the critical role of the information society, have not sufficiently influenced the protocol design[33].

45 The idea of collecting whatever information is available for as long as possible, (because "you never know when it might be useful") contravenes many data protection principles such as data quality (purpose limitation, necessity, proportionality, time limitation), lawfulness of processing, etc. It must be considered that the default configuration of many devices and software libraries, designed without awareness of data protection principles, might be based on a "maximum collection" approach. The configuration of such tools strongly influences the collection, processing and storage of available information at critical nodes of the ICT infrastructure, including web and applications servers, firewalls, and intrusion prevention and detection systems. Some of these systems can scan the very content of electronic communications to detect malware or other applications[34].

---

[33] In this regard considering and applying data protection by design and by default can help dealing with these shortages and risks (see Article 25 of the GDPR).

[34] One example of implementation of these "deep packet inspection" (DPI) mechanisms for incoming communications is the search for potential spam, scam and any form of unrequested or potentially harmful incoming e-mail. For DPI see e.g. http://en.wikipedia.org/wiki/Deep_packet_inspection .

46 Any such practices and systems, if not lawfully and fairly used, may lead to a thorough and comprehensive tracking of users' online behaviour and represent a threat to their fundamental rights and freedoms. Therefore, the configuration of such tools should be assessed and adjusted before they are used in EU institutions' web services.

5.2.2. Tracking technologies

47 Tracking can be defined as the action of associating users with their behaviour on the internet, such as visited web services and more detailed actions within those web services such as their clickstream, and processing all these data for various purposes.

48 Individuals can be identified not only via a set of natural identifiers like names, but through any set of parameters that would enable to single them out[35] and perform actions that have specific consequences on them.

49 Some tracking techniques are based on collecting unique identifiers directly entered by the user when interacting with the web service, such as user login accounts. Other unique identifiers are collected by the web service without the user's intervention, such as IP addresses, MAC addresses, mobile device identifiers, customer identifiers or cookies.

50 Other tracking techniques are linked to sets of web 'user agents' (typically web browsers) parameters transmitted by the web protocols to the web services when interacting with them, and are known as "browser (or any other user agent) fingerprinting" or "device fingerprinting" (see also section 4.2). These techniques can be used either alone or jointly with others to increase the level of precision of users' identification (due e.g. to a dynamic IP address because of DHCP protocol use) or as "bridge" solutions to cover situations where other identifiers, e.g. cookies, disappeared (for example because the user deleted existing cookies on their machine).

51 The use of smart mobile devices largely increases the opportunity for tracking users by adding other identifiers specific to mobile devices[36] and other sets of parameters, like location patterns and contextual data. These, alone or jointly with the identifiers mentioned above, offer effective tracking capabilities, often also presenting detailed personal information.

5.2.3. Profiling

52 Profiling is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to natural persons,

[35] Recital 26 of the GDPR gives singling out as an example of means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly. In this regard, see also WP29 Opinion 4/2007 on the concept of personal data and the further legal analysis and guidance on web tracking and profiling in Annex 1 of these Guidelines.

[36] Such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), Unique Device Identifier (UDI) and mobile phone number.

in particular to analyse or predict aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[37].

53 Tracking is a building block of profiling. The technical feasibility of associating users' behaviours to the same individual (see section 5.2.2), when using different on-line (and even off-line[38]) services in different places and times, together with the availability of adequate computing resources at affordable prices, enables what is called profiling."[39].

54 Profiling targets are websites visits or data exchanged by people browsing and interacting over the Internet (e.g. through e-mails or mobile apps), which could be used to build up a user's individual profile that be meaningful in specific contexts. This profile can then be used for a variety of aims, including taking decisions that could affect the individual concerned.

55 The purposes of profiling could be of a different nature, for instance, to optimise the architecture of one or more web services supporting the same business purpose, to find out consumers' preferences and serve targeted advertising, or to provide mobile users with contextual information. Profiles can also be built in areas like health, personality and performances, religious and political beliefs, social relationships, sexual orientation, financial situation, or physical location. If used unlawfully and unfairly, they could have serious consequences on people's freedoms and rights.

56 In some situations, there might be a need to only collect anonymous statistics on how people use on-line services, and profiling is used as an intermediate step before anonymisation. This type of operation constitutes processing of personal data, which carries risks, and as such needs to be addressed and managed.

5.3. Obligations, recommendations and best practices

57 If tracking is performed through "cookies" (as widely defined in section 4.2), what has been said in chapter 4 applies on top of what follows in this chapter. Some obligations, recommendations and best practices may overlap.

5.3.1. Legal basis and Data Protection Impact Assessment

R16: Above all EU institutions are reminded that, when planning possible tracking and profiling, they must always verify that these are grounded on a sound legal basis. The technical capability to perform these operations alone is not enough.

[37] Article 4(4) of the General Data Protection Regulation (see footnote 42)). See also WP29: Opinion 2/2010 on "online behavioural advertising": http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[38] "Big data" companies are increasingly combining information collected on-line and off-line to build larger and more accurate user profiles.

[39] WP29: "Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation", 13 May 2013

58 For risky processing operations such as those implying profiling, it is important to have a structured assessment of possible risks for the rights and freedoms of the individuals subject to these practices.

R17: The EU institution should perform a Data Protection Impact Assessment, at least limited to the profiling related purposes. If a prior check is required under Article 27 of the Regulation[40], the institution should annex the Data Protection Impact Assessment to the notification to the EDPS.

5.3.2. Privacy-friendly monitoring and logging capabilities

59 Since all logs containing IP addresses or other unique identifiers linked to the client side are considered personal data (see also Annex I for IP addresses), all obligations and safeguards for personal data apply[41].

60 Applying the principles of data protection by design and data protection by default is a good practice to ensure compliance with data protection principles, such as data minimisation, data quality, accuracy, fair processing and transparency. Adherence to these principles will become a legal obligation with the full applicability of the General Data Protection Regulation (GDPR)[42].

R18: The EU institution should analyse the default configurations of logging products and software libraries and limit the collection of information to what is strictly necessary for the purpose they serve[43].

R19: The EU institution cannot assume that consent once given by the user is valid forever and should give the user the possibility to review their decision, e.g. by periodically reminding them that they gave their consent to tracking and of what they consented to. This could be done at least every six months. In case of profiling this could be done more frequently.

[40] Verify in particular the applicability of Article 27(1)(c) of the Regulation.
[41] As an additional consideration, Article 11(1) of the GDPR states: "*If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.* ".
[42] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); OJ L 119, 04.05.2016, p.1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. Here we refer to Article 25 of the GDPR.
[43] For more detail see the forthcoming "Guidelines on the protection of personal data in IT governance and IT management of EU institutions"

5.3.3. Providing users with information on tracking and on how to make their choice on tracking

R20: The EU institution must be transparent and inform the user about the tracking and its purposes.

R21: Unless other conflicting reasons (such as security related ones) for denying wider transparency exist (in this case the DPO should always be involved in assessing this option), institutions' web services that track their users should provide them (directly or by a reliable reference) with any guidance on:

a. Tracking methods

b. How to express their decision on whether or not to be tracked when browsing the web service.

c. How to remove any tracking devices, for example cookies, previously set on their client device.

61

R22: If an external source is used to provide guidance, the institution should check that the information source complies with the EU data protection provisions and periodically verify the reliability of the information referenced.

5.3.4. What if a user enables the Do Not Track option on their user agent?

62 Nowadays many browsers support the Do Not Track[44] (DNT) option, which sends the web service a signal communicating that the client does not want to be tracked (see also same topic on section 4.3.3).

R23: Regardless of a browser's default setting of the DNT signal, in case the DNT signal expresses the user preference not to be tracked, as a precautionary measure, the EU institution should act accordingly and assume that the user has objected to the use of any tracking, as extended to both first and third party tracking mechanisms and to all purposes, unless an adequate and unambiguous use of the protocol explicitly indicates relevant exceptions or the explicit consent of the user has been collected in another way by any appropriate means, such as future additional protocols.

5.3.5. Data retention and need for anonymisation.

63 If data are not any longer necessary to be kept in an identified or identifiable form (personal data), then they must be either deleted or anonymised.

[44] W3C related standards, called Tracking Preference Expression, can be found at: http://www.w3.org/2011/tracking-protection/

For example, in case of analytics, personal data are aggregated for statistical purposes. The fact of being aggregated does not always ensure that they are completely anonymised. Checks are needed and original raw data are to be deleted.

R24: The EU institution must anonymise[45] personal data that are required as an intermediate step, but that do not need to be retained for the final purposes of certain processing operations such as anonymous analytics.

R25: The EU institution should use available standard techniques to perform effective anonymisation, consider re-identification risks, in particular when there could be serious consequences on people's freedoms and rights. No re-identification attempts must be performed.

R26: Pseudonymisation is not a measure equivalent to anonymisation (data resulting from them are still personal data and relevant obligations and recommendations still apply), but just a safeguard to mitigate risks.

5.3.6. Profiling users

64 For the private sector profiling is often used to accommodate their business model frequently based on monetising personal data for advertising purposes. The EU institutions should not use such models and only process personal data on a clear legal basis compatible with their role. . Profiling is highly intrusive to web service visitors' privacy and as such needs proper legal basis and adequate safeguards, if ever used.

R27: The EU institution must be transparent and inform the user about the profiling and its purposes. The EU institution should also provide transparency on profiling algorithms, unless other conflicting reasons exist (such as security related ones) to deny transparency. In the latter case the DPO should always be involved in assessing this option.

R28: The EU institution should consider providing the user with adequate means to enable the right of having any measure or decision based, even partially, on the profiling algorithm reconsidered with human intervention.

5.4. Further legal analysis and guidance

65 Some further legal insight and reasoning on tracking and profiling in the EU data protection framework, including the rights of the data subject in this processing and safeguards mitigating the risks posed by this processing, can be found in Annex 1.

[45] For more specific guidance on the subject see also WP29 Opinion 05/2014 on Anonymisation techniques: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

6. Processing by external organisations and transfers of personal data

6.1. General considerations

66 **These concepts are elaborated in the "Guidelines on the protection of personal data in IT governance and IT management". Some are repeated here to emphasize certain specific web services issues**.

67 Personal data collected by web services of an institution could be processed by organisations external to the institution[46] for two main reasons:

- either because the institution uses the services of a contractor or of any other external organisation to carry out its tasks;
- or because the institution sends these data to other organisations for purposes relating to the tasks and business of the latter.

68 In the first case the external organisation can be considered as a "**processor**" in the sense of Art. 2(e) of the Regulation. The Regulation defines a processor as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

An institution uses analytics services of an external company for their web services. The services are regulated by a contract and the company processes the personal data they collect to produce the statistics only as instructed by the institution. In this case the company acts as a processor.

69 In the second case the action of sending personal data to another organisation for its own purposes is defined as a "**transfer**" by Articles 7 and 8 of the Regulation. In this case the external organisation is a new controller, to whom data are transferred.

An institution features a web service to match offer and demand for job opportunities. The web service makes available APIs (programmatic interfaces) for stakeholders such as employers and centers for employment to get CVs of jobseekers. The institution thus performs a transfer of jobseekers' personal data to those stakeholders, under certain conditions.

70 Where data are made available to an external organisation outside the EU, irrespective of whether the recipient acts as processor or as new controller, the rules of Article 9 of the Regulation also apply. This means that at the time of choosing a non-EU based organisation, the EU institution will have to assess whether the level of personal data protection provided by the external organisation is adequate.

71 The Regulation requires **grounds for legitimacy and specific safeguards in both cases** (external organisation acting as processor or as new controller). Particular care

[46] For these guidelines, external organisations include other EU institutions or any other private/public organisation in or outside the EU.

should be taken in case of transfer of personal data to countries outside the EU/EEA and international organisations. More information on these grounds and safeguards can be found in the above-mentioned Guidelines.

R29: The EU institution must identify how the prospective involvement of external organisations fits in the Regulation (processor or new controller), consider grounds for legitimacy and needed safeguards.

72 The EU institution should **carefully evaluate the possible use of these third party components** in the context of an assessment of the data protection risks of the web service. In particular, the institution must pay attention to the issues of cookie management, information and transparency needs, need for consent, tracking, transfer of personal data to third parties and security, as described in this document.

R30: If the EU institution concludes that these grounds do not exist or the institution is not able to ensure the needed safeguards, they must explore other solutions, including the choice of different external organisation/services or the opportunity of performing those tasks internally.

R31: The EU institution needs to investigate whether the external organisation, further to processing personal data on their behalf, processes the institution's web service users' personal data also for their own purposes. In this case the organisation takes on the role of controller and relevant duties for those processing operations. The institution must verify the conditions for the transfer according to the Regulation.

This happens e.g. when an external organisation providing analytic services, or a social network whose functionalities are used by the EU institution to interact with their website users, process the personal data they collect from the institution also to make their own statistics or for behavioural advertising. In this case the institution performs a transfer of personal data to a new controller for those data and those purposes and must verify whether the conditions for the transfer exist.

This may also happen when the external organisation fails to act as data processor since it does not act strictly under the instruction of the controller or because it does not allow the controller to be in control of the security safeguards. If on the one hand, this does not exempt the institution from their own responsibilities, it puts, on the other hand, the chosen processor under scrutiny as a controller.

6.2. Tracking and profiling by third parties through components used by the institution's web service

73 Web services often include third party components like e.g. social plugins. These components may redirect the user towards the third party web services and send over (often using cookies to store it) personal information like e.g. the visited web service, when it was visited and other user agent information together with a user identifier that is unique for the third party web service and allows it to build a profile of the user.

R32: The EU institution should implement techniques that allow web services users to decide on using or not third party components and be in control before these components can redirect users to web services they did not request, and unlawfully transfer personal data, manage cookies and track users[47].

For example, certain social plug-ins forcing redirection when the page is loaded in the browser shall not be used. They can be replaced by links, or scripts can be developed to have those plug-ins in the webpage disabled by default and let users decide whether enabling them or not[48], once provided with clear info on the consequences of enabling them.

[47] If a third party service is essential and no alternative exists, the user may only have the choice not to use the EUI service. EUIs should strive to use third party services that are compliant with EU legislation.

[48] For an example of technical solution in that direction see this implementation: http://panzi.github.io/SocialSharePrivacy/.

7. Security obligations and recommendations specific to web services

7.1. General considerations

74 **General considerations on IT security management of institutions' web services in protecting user's personal data can be found in the "Guidelines on the protection of personal data in IT governance and IT management". Some are repeated here to enable emphasizing certain specific web services issues**

75 The institutions' IT infrastructures and web services, as many other governmental ones, have been the target of several cyber-attacks, some of which specifically addressed to them. In other cases specific web service vulnerabilities have been publicly disclosed that could have led to security incidents involving personal data.

76 Typical vulnerabilities include code injection, weak authentication mechanisms and unprotected channels to transmit credentials or sensitive data, bad configuration of servers and devices, mechanisms implying redirection of web clients to fraudulent sites or forcing unwanted requests on behalf of the victim[49].

77 This section recalls some high level recommendations and integrates some specific advice for web services, including guidance to protect personal data that could be at risk while implementing security measures.

7.2. Obligations, recommendations and best practices

7.2.1. Information Security Risk Management

78 One fundamental principle of data protection is the need to adopt security measures. Through an information security risks management process the EU institutions need to identify the relevant risks to the personal data processed through the web services they provide and then take appropriate organisational and technical measures to protect that personal data. Detailed advice on information security risk management can be found in the EDPS 'Guidance on information security risk management'.

79 The security measures produced by the information security risk management process will constitute part of the non-functional requirements of the planned web service. This process needs to be performed as soon as possible.

7.2.2. Secure web services development, operation and testing

R33: The EU institution should take into account known internet related threats and vulnerabilities, based on the specific web service architecture and technology.

[49] See for example: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project .

80 It is then very important to implement the identified security measures with the right technology. This implies staying abreast of new developments in threats and vulnerabilities, and their most effective countermeasures. This can be done in various ways including:

- Having security consultancy for the project.
- Using information sources like non-profit and commercial security projects. One of the most used free sources, for example, is the OWASP project[50], where the most common current threats and vulnerabilities for web services are described, together with possible countermeasures.
- Subscribing to the support services of the products (software (SW) and hardware (HW)) used, to receive vulnerability and threat alerts and relevant patches.
- Cooperating and liaising with the EU-Computer Emergency Response Team[51] whose aim is to support the institutions in protecting themselves against intentional and malicious attacks.
- Using IT security guidelines from ENISA[52] and advice and best practices of other EU institutions/departments with IT security specific expertise.

R34: The EU institution should have documented web service secure development, deployment, operation and security testing procedures following best practices. An essential role can be played by an integrated security testing approach in the development phase (with static code analysis and dynamic approaches such as penetration testing).

R35: The EU institution should provide relevant IT staff with adequate and up-to-date web service secure development, deployment, operation and security testing training.

7.2.3. Vulnerability management

R36: The EU institution should adopt and implement a vulnerability management process for SW and HW products used to secure its infrastructure from external threats.

81 Among relevant measures:

- An internal patching policy should be in place and documented.
- Patches need to be tested and deployed as early as possible.
- The choice of any product for the web service should also be guided by the provider's vulnerability management and patching practices.

[50] https://www.owasp.org/index.php/Main_Page
[51] http://cert.europa.eu/cert/plainedition/en/cert_about.html
[52] European Union Agency for Network and Information Security: http://www.enisa.europa.eu/

7.2.4. (Risks of) data breaches and relevant incidents

Current web services play also in a way the role previously played only by traditional telecommunications system. As a result, certain relevant rules apply in substance.

R37: The EU institution must comply with Article 35(2) of the Regulation which states that, in the context of an internal telecommunication network, "…in the event of any particular risk of a breach of the security of the network and terminal equipment", the institution "…shall inform users of the existence of that risk and of any possible remedies and alternative means of communication". The users to be informed are the staff of the institution and the authorised external users of the institution's web service[53].

R38: The same obligation applies substantially in case of established security breaches.

For example, if there is a high risk (or evidence) of hackers' compromise of a web service used by people to lodge complaints, the institution should publicly communicate the existence of this risk (or evidence) and advise on alternative ways (e.g. secure e-mail) to send those complaints.

R39: Of course, the EU institution may put in balance the public disclosure of the risk (or of the breach) and mainly its level of detail with possible disadvantages for the security of their web services and IT infrastructure. Any decisions taken in this context should be adequately grounded and documented.

7.2.5. Protection of personal data in transit: some basic advice for web services

R40: The EU institution must protect personal data sent over the Internet against risks to confidentiality, integrity and availability, including non-repudiation.

82 The institution needs to take into account threats such as, for example, "man in the middle" attacks[54], exploiting vulnerabilities like weak encryption.

R41: Use of adequate cryptographic solutions for confidentiality of internet communications and authentication of the web service is highly recommended.

[53] For further reasoning on the interpretation as recommended by the EDPS see Annex I.
[54] See e.g. https://www.owasp.org/index.php/Man-in-the-middle_attack

It is a commonly recognised good practice to use TLS protocol (over which internet protocols like HTTP can work[55]) with strong encryption algorithms to protect the communication between client and server side against eavesdropping and unauthorised alteration. The use of TLS should be coupled with a secure management of the relevant cryptographic keys and further safeguards[56]. This does not eliminate the risk but provides good reduction and should be among the safeguards for any category of personal data transmitted over the Internet.

7.2.6. Fair and lawful processing of personal data when managing the security of web services

83 The EDPS "e-Communication Guidelines"[57] focus on mechanisms and procedures to monitor unauthorised use of the Internet by institutions' staff. They contain many considerations that can also be extended to security measures for web traffic generated by connections to EU web services generated from outside the institution.

84 Security measures often involve the processing of personal information and thus should be adequate, relevant and proportionate considering on the one hand the identified security risks and on the other hand the data protection risks and compliance requirements. Access control, security monitoring and logging, and security incident follow-up procedures are, for example, among those countermeasures. Privacy enhancing security technologies and processes need to be explored and chosen when deciding on security countermeasures.

7.2.6.1. Security Logs

85 Considerations on processing of security logs for possible unauthorised use by the staff of the institution can be found in the EDPS e-Communication Guidelines. Nevertheless, the institutions perform also actions to protect web services against unauthorised use by external users.

R42: Logs created only for the security and control of the web service may not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences, according to Article 6(2) of the Regulation.

[55] HTTP over SSL/TLS is known as HTTPS

[56] Such as obliging the web client to use HTTPS through "HTTP Strict Transport Security" or to mitigate the consequences of a compromise of some cryptographic keys through the so called Forward Secrecy.

[57] Guidelines on personal data and electronic communications in the EU institutions, EDPS, December 2015 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-16_eCommunications_EN.pdf

R43: Furthermore, under Article 37 of the Regulation, Internet communication traffic logs collected by the institutions' infrastructure and used to verify the authorised use of the communication system *"…shall be erased or made anonymous as soon as possible and no later than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court*". In the latter case, the controller is accountable for the need for a retention time longer than six months and file the relevant justification.

R44: Monitoring and logging of traffic interacting with institutions' web services for security and traffic management, usually performed by networking equipment such as routers, hubs, switches, firewalls and intrusion prevention and detection systems, should collect and process only the information necessary, adequate and relevant for the purposes they serve. The proportionality must be ensured at each stage of the operations, in particular at log generation.

7.2.6.2. Incident management

R45: The EU institution should limit processing of personal data in the context of an incident management procedure, such as recording information about the incident or informing other institutions, CERTs, security consultants or the public, to what is strictly necessary for a successful incident follow-up.

R46: In case of doubts on the necessity of disclosing certain information, the EU institution should consider step-by-step and proportional disclosure.

R47: Once a choice of personal data to be disclosed is made, institutions need to protect the information from unfair and unlawful use, which includes setting up transparent procedures.

7.2.6.3. Use of personal data in testing activities

86 The development and testing environments by their own nature usually contain less safeguards, in particular as to how and under which conditions the test data should be used.

87 This is why using production data for testing purposes increases the risk of an unauthorised access and modification. Furthermore, using production data for testing means that the data are used for a different purpose than the one for which they were collected. The EU institution must therefore keep in mind the compliance with the Regulation and act accordingly. In exceptional cases, if a certain situation cannot be reproduced, production data may be used under strict conditions.[58]

[58] In this respect, see the European Commission Standard on secure systems development as an example of the conditions defined by an EU institution for the use of production data for testing purposes in its systems.

R48: No 'production' data[59] should be used for testing. If generating random yet appropriate test data sets proves a disproportionate effort then adequate techniques for creating synthetic, anonymised data using some production data as a starting point should be used.

R49: In case of bugs in system operation, the use of "production" personal data for code debugging should be avoided. In any case, if needed, an authorisation from the data controller (or any staff member accountable to the controller for that processing operation) needs to be obtained and both the authorisation process and the debugging actions need to be recorded and auditable. The amount of personal data used for testing should anyhow be minimised and a strict "need to know" policy applied. The DPO should be consulted.

7.2.6.4. Anonymous browsing of institutions' web services

88 Certain proxy services are used by people to browse the Internet without exposing their own source IP address and thus strongly reducing the risk of identification (this is known as "anonymous browsing"). This practice can be useful to avoid any unlawful surveillance for citizens who are bound to use infrastructure located in countries with a low democratic profile or for risky activities like investigative journalism.

R50: Definitively prohibiting web service connections coming from those proxy services for security reasons is not a good practice when there is no evidence that the measure is relevant (no evidence of former threats or low probability of effective attacks from those services), necessary (alternative techniques might exist to block certain traffic) and proportional (e.g. temporary ban based on some preliminary evidence could be chosen against generalised definitive ban).

[59] Data actually processed by the web service during its normal operations.

Annex 1. Further legal analysis and guidance

89 This Annex provides some further legal insight and reasoning to support the guidance given in the chapters, without aiming at being exhaustive.

Personal data processed via a web service

IP addresses as personal data

90 The WP29 has discussed the status of IP addresses as personal data in its Opinion no. 4/2007 on the concept of personal data[60]. This classification has also been the subject of cases at the Court of Justice of the European Union[61]. In practice, IP addresses are not processed in isolation, but in combination with other attributes which provide additional possibilities for the identification of the individual to which the record relates, either by the controller or by another entity that may obtain access to this record. The EU institution must apply the precautionary principle and always protect records containing IP addresses as personal data.

Consent as a legal ground for lawful processing

91 When using consent as a legal ground for processing, the EU institution should consider the following issues:

- Consent validity: the consent of the data subject to the processing of his or her personal data needs to be freely given, unambiguous, specific and informed to be valid. According to WP29[62], consent should include a clear indication of the data subject's decision, which will include proactive confirmation on their part. The consent is valid only when the data subject exercises a real choice and a voluntary and specific decision.
- Processing of sensitive data: as defined in Article 10 of the Regulation, consent is a valid legal basis except where internal rules adopted by the institution does not allow it.[63]

---

[60] WP29 Opinion 4/2007 on the concept of personal data: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[61] Case C-70/10 Scarlet Extended SA: *"Those addresses are protected personal data because they allow those users to be precisely identified"* (paragraph 51); Case C-582/14 Breyer: "*Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services … constitutes personal data … where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person*" (paragraph 49).

[62] See WP29 Opinion 15/2011 on the definition of consent: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[63] See Article 10(2)(a) of the Regulation.

- Freely given consent: conditions for a free consent should be carefully verified, given that the public authority status of the EU institution may call into question the validity of the consent of the data subject.
- Furthermore, in case of consent as a legal basis, the institutions need to set up facilities for obtaining a valid consent, otherwise the legitimacy of the processing is compromised.
- Implied consent: such a consent - inferred from an action or inaction (lack of response) of an individual - is valid only when it is possible to ascertain, without any doubt, from their actions that individuals have agreed to the transaction[64]. Implied consent inferred by a lack of response of the individual is not valid.
- In case of consent as a legal basis for certain types of cookies, see relevant topics in chapter 4.

Consent and information to users for cookies and other client side techniques

Processing personal data through cookies and similar technologies: applicability of Regulation 45/2001

92 Regulation 45/2001 applies to any personal data processing operations carried out by EU institutions and thus also to cookies.

93 Cookies can contain parameters uniquely identifying the terminal equipment they are created on and, in practice, the individual using that device. Even when they do not contain identifiers, they can collect data from the user's device which could be attributed to a terminal device and to an identified or identifiable individual when linked with other parameters, such as IP addresses (see also above). As such, at least as a precaution, the institutions should always treat cookies as personal information and protect them accordingly.

94 Tracking cookies (see also section 5.2.2) are used to track users' online behaviour in order to perform actions on those particular users (singling out). As a result, tracking cookies are personal data as defined in the Regulation, even if the traditional identity parameters (name, address, etc.) of the tracked user are unknown or have been deleted by the tracker after collection.

The applicability of the ePrivacy Directive

95 Recitals 10 to 12 of the Regulation determine its relationship to the other data protection instruments of the Union acquis. They refer to Directive 97/66/EC and Directive

[64] In this regard, see WP29 Opinion 15/2011 on the definition of consent (op.cit.), pages 24 and 25.

95/46/EC and "various other Community measures" which are "*designed to specify and add to Directive 95/46/EC in the sectors to which they relate*". As Recital 12 confirms, these references need to be read in the context of the objective that "*consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data should be ensured throughout the Community*."

96 Article 19 of the ePrivacy Directive 2002/58/EC repeals Directive 97/66/EC and provides that "*References made to the repealed Directive shall be construed as being made to this Directive [2002/58/EC]*". This also applies to the reference in Recital 10 of the Regulation.

97 Furthermore, the obligation to ensure consistent and harmonious application of the acquis throughout the Union would mean that the EU institutions should apply the same rules as any other entity covered by Union law unless there are reasons relating to their nature that require a different regime. Such different conditions would require to be laid down explicitly in specific legislation, as it is indeed the case for some provisions of the Regulation. No such reasons can be seen to allow EU institution web services other rights with respect to user terminals than any other entity.

98 Following these considerations, there is no ground to argue that the interactions of EU institutions with user devices should follow different rules than all other entities covered by Directive 2002/58/EC. They should therefore apply the principles laid down in Article 5(3) of Directive 2002/58/EC when providing web services.

What should be considered under the scope of Article 5(3) of the ePrivacy Directive

99 In line with the text of the Article, the scope will include any technology which enables the reading or storing of web service information from/onto the users' devices (see section 4.2). In line with the text of the Article, the information accessed or stored does not need to be personal data.

Need for consent

100 According to the Article 5(3), the use of cookies *"is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing"*.

101 Article 5(3) provides for two exceptions to this rule:

- when the cookie is used "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network*" or
- when the cookie is "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

102 These exceptions have been extensively analysed by the WP29 Opinion 04/2012 on Cookie Consent Exemption[65]. The controller needs to perform an assessment for the specific use of cookies to understand their purpose and thus whether one of the exceptions applies, using the guidance provided by the WP29's Opinion.

103 Tracking cookies from social plug-ins, third party advertising and analytics clearly require prior and informed consent. Even first party analytics, as the WP29 says, while "*… they are often considered as a "strictly necessary" tool for web service operators, they are not strictly necessary to provide a functionality explicitly requested by the user*", are not exempted.

104 In the same Opinion the WP29 suggests that a possible third exemption could be set out in the future by the legislator[66] in specific circumstances. The EDPS believes that under very strict conditions this exemption may be granted in substance due to the low risk for individuals as also balanced with advantages for the institutions[67]. This exemption and relevant conditions are described in section 4.3.1.

Prior consent

105 When consent is needed, it needs to be collected before any read/write operation on the terminal equipment is carried out, i.e. before cookies are set. All essential elements of valid consent should be present at that time.

Informed consent

106 An essential element of consent is the information provided to the user. The type and accuracy of the information provided needs to be such as to put users in control of the data on their device.

---

[65] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[66] See WP29 Opinion 4/2007 on the concept of personal data (op.cit.), page 10: "*However, the Working Party considers that first party analytics cookies are not likely to create a privacy risk when they are strictly limited to first party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards. Such safeguards are expected to include a user friendly mechanism to opt-out from any data collection and comprehensive anonymisation mechanisms that are applied to other collected identifiable information such as IP addresses.*
In this regard, should article 5.3 of the Directive 2002/58/EC be re-visited in the future, the European legislator might appropriately add a third exemption criterion to consent for cookies that are strictly limited to first party anonymized and aggregated statistical purposes.
First party analytics should be clearly distinguished from third party analytics, which use a common third party cookie to collect navigation information related to users across distinct websites, and which pose a substantially greater risk to privacy".

[67] In its Preliminary Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC) of 22 July 2016 the EDPS supports the creation of this additional exemption (p. 17).

Other conditions for valid consent

107 In the light of the above, all requirements of a valid consent apply to cookies[68] [69]. Users have to be given the option to change their wishes and revoke their decision at any time. In particular the consent should be:

- Specific. The information provided to the user should highlight the link between cookies and the type of data processed through them, along with any related purposes. This also implies a granularity in the options for consenting to one cookie rather than another, with data types and associated purposes as distinguishing factors.
- Expressed through an active choice[70]. The procedure and tools used to obtain consent should allow users to express their wishes, with no margin of doubt about what their decision is. As such, those procedures and tools need to make sure that users actively confirm that they have been informed clearly and comprehensively about the way that their data will be processed, and that they fully consent to this.
- Freely given. Users should be given the opportunity to make a real choice in accepting or declining cookies, e.g. without being put under pressure or presented with a "take it or leave it" approach.

Web tracking and profiling

Tracking and profiling in the EU data protection framework

108 Tracking as such involves an immediate identification or singling out of the data subject without even necessarily considering other means likely reasonably to be used either by the controller or by any other person[71]. As a result this implies a straightforward application of the whole Regulation.

109 Regulation 45/2001 does not contain the notion of "profiling". The GDPR defines profiling in Article 4(4). Profiling is most relevant in the context of automated decisions, as addressed by Article 22 of the GDPR. Analogue considerations can be made for Article 19 of the Regulation.

---

[68] See WP29 Opinion 2/2010 on online behavioural advertising (op.cit.) and Opinion 16/2011 on "the EASA/IAB Best Practice Recommendation on Online Behavioural Advertising": http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf .

[69] Art. 2(h) and 5(d) of the Regulation

[70] See WP29 Working Document 2/2013 providing guidance on obtaining consent for cookies : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

[71] See also Recital 26 of the GDPR.

110 Some consequences of profiling are also dealt with by Article 19 of the Regulation, which gives data subjects the right not to be subject to decisions which are based solely on automated processing operations, if the decision has legal effects or otherwise significantly affects them.

111 Moreover, Article 13(d) of the Regulation adds another element to the right of access in the case of automated decisions concerning a data subject. In particular, it grants the data subject the right to obtain from the controller knowledge of the logic involved in any automated decision process. This actually means that the data controller/ institution is obliged to provide the data subject with the requested information, even though the decision might not have legal or other significant effects on them.

112 For what is not specified, profiling processing operations are covered by all provisions and safeguards in the Regulation.

113 The analysis of the WP29 suggests focussing on the following aspects, aimed at mitigating the risks posed by profiling:

- Greater transparency for data subjects, entailing additional information requirements for data controllers.
- A sound legal basis, such as Union law or consent (where all the conditions for a valid consent are met, as outlined in Annex 1) and the exclusion of the individual's automated evaluation based on special categories of data as listed in Article 10 of the Regulation.
- Clear data subject's right to access, modify or delete the profile information and refuse any measure or decision based on it or have them reconsidered with human intervention.
- More accountability for controllers (and processors). It is recommended that Data Protection Impact Assessments be carried out to mitigate specific profiling related risks through adequate safeguards, which include a strict data protection by design and by default and data minimisation approach.[72]

[72] While this is still not mandatory under the Regulation (EC) No 45/2001, it will be mandatory when the Regulation (EC) No 45/2001 will be adapted to the GDPR. In any case, this is considered a good practice.

Security

Information to data subjects on (risks of) data breaches and relevant incidents

114 The obligation to inform the user of the risk of a breach in accordance with Article 35(2)[73] of the Regulation was originally thought as addressed to the staff of the EU institutions. Nevertheless it should be interpreted more widely as directed also to the authorised external users of the EU institutions' web services.

115 Article 34 of the Regulation indeed specifies that "*'user' shall mean any natural person using a telecommunications network or terminal equipment operated under the control of* ..." an EU institution. Hence an obligation exists for the institutions to notify also external users of such risks for online services enabling data subjects to "communicate" with the institutions in a confidential way and to inform them on remedies and other ways to communicate securely with the institutions.

116 While the obligation exists for risks, the Regulation does not offer any explicit provisions for established security breaches. Nevertheless, the rationale behind Article 35(2) implies at least the same obligation in that event.

[73] "In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication."

Annex 2. Glossary

Expression	Explanation
Cache	Web caches are local or network resources providing storage and retrieval of information on previous web activity to increase computing performances.
Cookie	Strictly defined they are pieces of text generated by the web services that the user has visited. Web services store these text files on the devices where the web browsers are installed to enable the exchange of information.
Controller	The EU institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of processing personal data.
Data subject	An identified or identifiable natural person to whom personal data relate. He/she could be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
IP address	A unique string of numbers that identifies each computer using the Internet Protocol to communicate over a network. E.g.: 210.100.147.166
Log	A file containing a sequence of events that are useful to understand how the system it relates to has been used.
Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Profiling	Any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, preferences, interests, reliability, behaviour, location or movements.
Proxy	A network application acting as an intermediary on exchanges over the internet. Web proxies are often used to facilitate the access to internet resources and provide mitigation on identifiability via a different IP address than the originating one.
Script	A (piece of) computing program conceived in a way to exploit language interpreters (themselves software programs) available to the computing machine. Scripting languages are commonly used for web programming.
Threat (IT security)	An individual, an application or any other agent that exploits a weakness to compromise the security of an application or a system.
Tracking (online)	Monitoring and keeping a record of a user's online activities.
Vulnerability (IT security)	A weakness in an application or a system which allows an unauthorised individual or system to reduce the affected system's information assurance.
Web service	Any type of information service made accessible over the Internet.. "Mobile" web services, which are designed to be better accessed by smart mobile devices via mobile browsers, are included.