DETAILED INSPECTION PLAN (DIP)

ON

INSPECTION PURSUANT TO ARTICLE 47 (2) OF REGULATION (EC) N. 45/2001

IT system concerned:

Web services managed by the European Institutions and Bodies

EDPS case number 2017-0632

EDPS
IT Policy Sector and Supervision & Enforcement Unit

Contents

1. ORIGIN OF CASE AND OBJECTIVES OF THE INSPECTION

The decision to carry out a thematic targeted inspection was determined by taking into account the following points:

- Article 46 b) of the Regulation stipulating that "*The European Data Protection Supervisor shall: (b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;*" and
- Article 46 c) of the Regulation stipulating that "*The European Data Protection Supervisor shall: (c) monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;*"

Websites process personal data, e.g. for analysis of their use. They use internal functions and may use third-party components, such as embedded YouTube videos or social media buttons, to enrich the experience of the web service. These processing practices introduce data protection obligations to be implemented by the web service controller. This inspection will evaluate the compliance of web services provided by European Institutions with respect to first-party and third-party tracking.

2. SCOPE

This thematic targeted inspection assesses the alignment of web services of the European Institutions and Bodies (EUI) with Regulation 45/2001/EC and Directive 2002/58/EC. For the practical implementation, the EDPS' recommendations made in the "Guidelines on the protection of personal data processed through web services provided by EU institutions" ("the web services guidelines")[1] will provide a standard. This inspection aims to carry out automated remote tests on all EUI web services publicly accessible via the HTTP or HTTPS protocol that provide HTML pages for individuals (hereinafter *EUI HTML web services*). Based on preliminary findings, a subset of those web services is selected to pass a manual remote examination using a subset of recommendations from the web services guidelines given in Annex 2.

Social network and collaboration platform services are only registered by their URL to assess the extent of use by EUI, but are otherwise not considered in this inspection.

The scope of the inspection comprises:

- The existence and accuracy of a privacy policy, cookie notices or similar policy documents (R3, R5, R6, R7,R9, R11, R19, R20, R23,)
- The security of the personal data in transit between the Web Service and the terminal equipment of a data subject (HTTPS) (R32, R33, R40, R41)

3. METHODOLOGY

Within 15 days of reception of the announcement notice, all EUI must provide the EDPS with an exhaustive list of their EUI HTML web services to whom they are controller or co-controller, and usage

[1] https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_web_services_en.pdf

statistics, if collected[2]. Due to the expected high number of web services, the inspection is carried out in several phases ("waves") of which each covers a subset of web services.

The first wave consists of a subset[3] of already identified EUI HTML web services listed in Annex 1. The EDPS selects the subset taking into account the expected impact of any possible lack of compliance (number of visitors, types of personal data processed and size of the web service) and records the choice in the inspection minutes. *Intermediate reports* are produced for each wave and a *final report* concludes the web services inspection. All EUI are provided with report sections on EUI HTML web services to whom they are controller or co-controller and generic sections on overall observations and recommendations.

The EUI controller will be notified about the inspection of its EUI HTML web service two weeks before the remote evidence collection. The controller should not alter parts of the web service that may impact the inspection outcome, e.g. web service policies or cookie configuration, during the collection period i.e. within two weeks from the announced data of the starting of the evidence collection.

The remote inspection is carried out for each EUI HTML web service individually and comprises two parts. The *first part* is automated and collects evidence from which overall statistics are produced and possible data protection issues are identified. Depending on the severity of data protection issues supported by these findings, a *second part* may follow in which further evidence is researched for a later manual evaluation. Inspection steps and collected evidence are documented in *minutes*. The minutes are prepared for each EUI HTML web service at the EDPS premises and submitted electronically to the respective web service controllers for optional comments. Comments provided within three weeks are considered by the inspection team. If no comments are provided within the deadline, the minutes are considered final. The inspected EUI will be sent a copy of the final minutes for signing and might request a copy of all the files with the collected evidence.

The final minutes and evaluation results are compiled into intermediate reports for each EUI in each wave. The report contains a first part with main findings common to all web services and a second part which is web service specific.

After each wave, the EDPS will send to the management of each EUI the common part and the specific part concerning the respective EUI. The intermediate report shall be signed and returned to the EDPS within 15 days of reception to acknowledge receipt by the management (or representative) of the inspected EUI.

The inspection is performed in accordance with the procedures established in the EDPS Inspection guidelines with the exceptions as described in Section 4.

3.1. Automated Remote Evidence Collection

The automated remote evidence collection considers only the state of the web service with no other interaction than browsing by clicking HTML links, hence without consenting or rejecting the use of cookies or other similar devices for any purpose. The collection for each web service includes:

---

2 The information should provide high level usage statistics for a reference period determined by the EUI. Daily, monthly, annual numbers of visits (or unique visitors) are acceptable. The type of data should be explained.

3 The EDPS choses the subset taking into account the expected impact of any possible lack of compliance (number of visitors, types of personal data processed and size of the web service) and records the choice in the inspection minutes.

1) screenshot of the English web service home page (after language selection)
2) full-text of web service home page if response is HTML
3) list with labels and URLs of HTTP links accessible from the home page
    a) within the host and path of the web service's home (*child links*),
    b) all others *(other links*), and
    c) those linking to widely used social networks and collaboration services (*social network links*)
4) random HTML links as a subset of 3.a) including the home webpages used for browsing and alongside collection of traffic and persistent data, in particular
    a) recording of information exchange with the browser and other hosts,
    b) information stored in HTML5 local storage[4],
    c) list with first- and third-party persistent cookies,
    d) list with prospective first- and third-party tracking requests (web beacons[5], etc.),
    e) list of requested third-party hosts and others such as subdomains to web service, and
    f) list of requests identified by the EasyList filter[6] to cause user tracking
5) information regarding the use of SSL encryption, i.e.
    a) availability of HTTPS for web service host,
    b) setup of redirect for HTTP requests to home page, and if, redirect location, and
    c) list of known vulnerabilities of the employed SSL setup

Furthermore, two tables are populated with a row for each link in 3.a), respectively 3.b), that have either in the caption or URL a keyword listed in Annex 3. For every row, caption and URL, detected keywords, and the HTML webpage's title, first-party cookies and local storage are listed. In case of a subsequent manual examination, both tables help the inspection team to find relevant webpage for a legal assessment.

3.2. Criteria for Manual Evidence Collection and Manual Evaluation

The inspection team selects web services for a manual evidence collection[7] and manual evaluation based on the following non-exhaustive list of criteria:

- number of third-party cookies, web beacons and HTML5 local storage entries,
- number of requested third-party hosts,
- excessive cookie retention periods, and
- extent of use of social network and collaboration platforms
- web service visitor statistics, if available

[4] Local storage allows web pages to read from and write to a persistent browser data storage.

[5] see https://en.wikipedia.org/wiki/Web_beacon (accessed 24/04/2018 at 19:04)

[6] See https://easylist.to/#easyprivacy.

[7] Most if not all the recommendations of annex 2 cannot be checked without manual evidence collection and evaluation.

3.3. Manual Evidence Collection

The remote manual evidence collection includes for each web service:

- copy of the cookie notice,
- details of consent mechanism (e.g. banner, footer, overlay and provided information),
- copy of the cookie policy, and
- copy of the privacy policy

3.4. Manual Evaluation

Based on the final minutes, the remote manual evaluation assesses:

- adequacy of the privacy-related legal documents used to inform visitors,
- existence and form of a cookie consent mechanism, and
- purpose of detected cookies, web beacons and HTML5 local storage entries, their necessity, and the suitability of their retention periods

To ensure an efficient inspection, the manual evaluation is carried out on a best-effort basis and not necessarily exhaustive. It may be suspended if clear compliance issues, such as use of third-party tracking cookies with no legal basis, are found.

3.5. Inspection Minutes

The inspection minutes for each web service consists out of the inspection steps, the automatically collected evidence according to 3.1 and, if carried out, the manually collected evidence according to 3.4.

Automatically collected evidence will be provided in the form of:

- HTTP Archives (*.har) recorded during the automated browsing. As these files record all the content of the visited webpages, they may contain personal data and shall not be archived longer than necessary for the purpose of this inspection.
- A structured plain-text file (*.yml) containing the relevant items detected during the tests
- A document describing the previous file structure.

3.6. Intermediate and Final Reports

The intermediate report of each wave contains a first part with main findings common to all web services and a second part which is web service specific. After the last wave of web service inspections, a final report is compiled on the basis of all intermediate reports.

Web service specific report parts will include:

a) General considerations and recommendations

b) An analysis section listing the relevant findings. Each finding will contain the following sections:
   - Background and Criteria
   - A findings section containing the evidence leading to the conclusions.
   - Feedback of Web Service Controller (when applicable)
   - Conclusions describing the infringements found, if any.
   - Recommendations on how to address the infringements found, if any.

c) List of recommendations with a deadline for each.

4. DEROGATIONS FROM THE INSPECTION CASE MANUAL

The EDPS Inspection Case Manual does not contain explicit provisions for remote inspections, so that few derogations must be introduced. Remote inspections do not require a visit of the actual premises of the institution. Consequently, "on-the-spot" is interpreted as navigating or crawling the online web service. The following steps are omitted or adjusted for the indicated reason.

4.1. Derogation from 6.1.1.3 General preparation prior to the on-the-spot operation

No information has been requested in advance as a subset of web services is already known to the EDPS to start with.

4.2. Derogation from 6.1.1.5 Practical arrangements

No travel and hotel arrangements have been made and no mission order has been introduced in the MIPS application as the involved Staff members will not be required to leave the EDPS premises.

4.3. Derogation from 6.1.1.6 Detailed inspection plan (DIP)

The interview section has been omitted as no interviews will be required to perform this inspection.

This Section 4 has been introduced to record the derogations.

4.4. Derogation from 6.1.2.2 Kick-off meeting

No Kick-off meeting will be held as the cooperation of the European Institution or Body is not required and no visit of said Institution or Body is required.

4.5. Derogation from 6.1.3.2.4 Finalisation and submission of the minutes

The evidence is collected from the EUI html web service. As there are only very small margins for interpretation during this phase and to avoid unnecessary delays, the inspected institution is only given the opportunity to sign the final minutes on explicit request in the timely submitted comments on the minutes.

ANNEX 1: WEBSITE LIST[8]

General EU portal

- European Union Portal europa.eu

Institutions and Bodies

- European Parliament (EP) www.europarl.europa.eu
- European Council / Council of the European Union (Council) www.consilium.europa.eu
- European Commission (EC) ec.europa.eu
- Court of Justice of the European Union (ECJ) curia.europa.eu
- European Central Bank (ECB) www.ecb.europa.eu
- European Court of Auditors (ECA) eca.europa.eu
- European External Action Service (EEAS) eeas.europa.eu
- European Economic and Social Committee (EESC) www.eesc.europa.eu
- Committee of the Regions (CoR) cor.europa.eu
- European Investment Bank (EIB) www.eib.org
- European Investment Fund (EIF) www.eif.org
- European Ombudsman (EO) www.ombudsman.europa.eu
- European Data Protection Supervisor (EDPS) edps.europa.eu

Services, agencies and joint undertakings

- Joint Research Centre (JRC) ec.europa.eu/jrc/
- Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) cert.europa.eu
- European Personnel Selection Office (EPSO) epso.europa.eu
- European School of Administration (EAS) europa.eu/eas/index_en.htm
- European Publications Office (PO) publications.europa.eu
- Agency for the Cooperation of Energy Regulators (ACER) www.acer.europa.eu
- Community Plant Variety Office (CPVO) cpvo.europa.eu
- Eurojust - the European Union's Judicial Cooperation Unit (Eurojust) eurojust.europa.eu
- European Agency for Safety and Health at Work (EU-OSHA) osha.europa.eu
- European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) www.eulisa.europa.eu

[8] The EU institutions, agencies, bodies, joint undertakings and interinstitutional services as listed in the Interinstitutional style guide http://publications.europa.eu/code/en/en-390500.htm

- European Asylum Support Office (EASO) www.easo.europa.eu
- European Aviation Safety Agency (EASA) www.easa.europa.eu
- European Banking Authority (EBA) www.eba.europa.eu
- European Border and Coast Guard Agency (Frontex) frontex.europa.eu
- European Centre for Disease Prevention and Control (ECDC) ecdc.europa.eu
- European Centre for the Development of Vocational Training (Cedefop) www.cedefop.europa.eu
- European Chemicals Agency (ECHA) echa.europa.eu
- European Environment Agency (EEA) www.eea.europa.eu
- European Fisheries Control Agency (EFCA) www.efca.europa.eu
- European Food Safety Authority (EFSA) www.efsa.europa.eu
- European Foundation for the Improvement of Living and Working Conditions (Eurofound) www.eurofound.europa.eu
- European GNSS Agency (GSA) www.gsa.europa.eu
- European Institute for Gender Equality (EIGE) www.eige.europa.eu
- European Insurance and Occupational Pensions Authority (EIOPA) eiopa.europa.eu
- European Maritime Safety Agency (EMSA) www.emsa.europa.eu
- European Medicines Agency (EMA) www.ema.europa.eu
- European Monitoring Centre for Drugs and Addiction (EMCDDA) www.emcdda.europa.eu
- European Securities and Markets Authority (ESMA) www.esma.europa.eu
- European Training Foundation (ETF) www.etf.europa.eu
- European Union Agency for Fundamental Rights (FRA) fra.europa.eu
- European Union Agency for Law Enforcement Cooperation (Europol) www.europol.europa.eu
- European Union Agency for Law Enforcement Training (CEPOL) www.cepol.europa.eu
- European Union Agency for Network and Information Security (ENISA) www.enisa.europa.eu
- European Union Agency for Railways (ERA) www.era.europa.eu
- European Union Intellectual Property Office (EUIPO) euipo.europa.eu/ohimportal
- Office of the Body of European Regulators for Electronic Communications (BEREC Office) berec.europa.eu
- Single Resolution Board (SRB) srb.europa.eu/
- Translation Centre for the Bodies of the European Union (CdT) cdt.europa.eu
- European Defence Agency (EDA) www.eda.europa.eu
- European Union Institute for Security Studies (EUISS) www.iss.europa.eu
- European Union Satellite Centre (Satcen) www.satcen.europa.eu
- Consumers, Health and Food Executive Agency (CHAFEA) ec.europa.eu/chafea
- Education, Audiovisual and Culture Executive Agency (EACEA) eacea.ec.europa.eu
- European Research Council Executive Agency (ERCEA) erc.europa.eu
- Executive Agency for Small and Medium-sized enterprises (EASME) ec.europa.eu/easme

- Innovation and Networks Executive Agency (INEA) ec.europa.eu/inea
- Research Executive Agency (REA) ec.europa.eu/rea
- Euratom Supply Agency ec.europa.eu/euratom
- Fusion for Energy Joint Undertaking (F4E JU) fusionforenergy.europa.eu
- Bio-based Industries Joint Undertaking (BBI JU) www.bbi-europe.eu/
- Clean Sky 2 Joint Undertaking (CSJU) cleansky.eu
- ECSEL Joint Undertaking (ECSEL JU) www.ecsel-ju.eu
- European Institute of Innovation and Technology (EIT) eit.europa.eu
- Fuel Cells and Hydrogen 2 Joint Undertaking - (FCH 2 JU) www.fch.europa.eu
- Innovative Medicines Initiative 2 Joint Undertaking - (IMI 2 JU) www.imi.europa.eu
- SESAR Joint Undertaking - (SESAR JU) www.sesarju.eu
- Shift2Rail Joint Undertaking (Shift2Rail JU) shift2rail.org/

Non EU Organisations under EDPS' supervision

- EFTA Surveillance Authority www.eftasurv.int/

ANNEX 2: RECOMMENDATION LIST

Recommendation	Description
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.
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.
R6	A layered approach, where the information is given at different stages providing greater detail, should be used. Nevertheless, the essential information should be present at a sufficient level of detail to put the user in control already at the first layer.
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
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).
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.
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.
R20	The EU institution must be transparent and inform the user about the tracking and its purposes.
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.
R33	The EU institution should take into account known internet related threats and vulnerabilities, based on the specific web service architecture and technology.

12

Recommendation	Description
R40	The EU institution must protect personal data sent over the Internet against risks to confidentiality, integrity and availability, including non-repudiation.
R41	Use of adequate cryptographic solutions for confidentiality of internet communications and authentication of the web service is highly recommended.