Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament

The European Data Protection Supervisor,

Having regard to the Treaty on the functioning of the European Union,

Having regard to Article 58(2)(b) and (e) of Regulation (EU) 2018/1725,

Has adopted the following decision:

PART I - Proceedings

On 29 October 2020, the European Data Protection Supervisor ('the EDPS') received a complaint under Article 68 of Regulation (EU) 2018/1725 (the Regulation)[1] jointly signed by Members of the European Parliament ('MEPs') [redacted] (the complainants), against the European Parliament (the Parliament), regarding alleged infringements of Article 15 and Chapter V of the Regulation through one of the Parliament's websites. The complaint was registered under case 2020-1013.

Following receipt of the complaint, the EDPS started investigating it pursuant to Article 57(1)(e) of the Regulation. In this context, on 9 December 2020, he contacted the Parliament's Data Protection Officer ('DPO') inquiring about progress in the handling of a complaint concerning the same subject, which had been previously submitted to the Parliament by the complainants. The Parliament's DPO replied on 17 December 2020.

On 20 January 2021, the EDPS followed up on this correspondence in order to bring the DPO's attention to some issues relating to the data protection notice(s) published on the website http://europarl.ecocare.center (the dedicated website), and inquired about the purpose of a unique identifier (uid) stored on the website together with a cookie.

On 22 January 2021, the EDPS received, under Article 67 of the Regulation, a complementary complaint to the one registered under case 2020-1013 by the non-profit organisation noyb – European Center for Digital Rights ('noyb'). This complaint established the representation of the complainants by noyb, repeated the main allegations of the original complaint, and expanded on it with additional information and arguments. On 29 January 2021, MEP [redacted]

[1] Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

[redacted] joined the complaint, providing a mandate for her representation by noyb. Since the 29 October 2020 and 22 January 2021 complaints have the same subject matter, they have been handled under the same case file.

In reply to the EDPS's communication of 20 January 2021, the Parliament's DPO service informed the EDPS on 4 February 2021 that most of the identified issues had been solved and that the text of the data protection notice had been updated on the website, without, however, providing further information on the exact changes implemented.

The EDPS continued the examination of the complaint pursuant to Article 57(1)(e) of the Regulation, and invited the Parliament to comment on the allegations brought forward by the complainants and their representative, noyb, by letter dated 16 February 2021.

The Parliament replied on 25 March 2021. The EDPS requested on 31 March 2021 the complainant's comments on the Parliament's reply, which he received on 20 May 2021. The EDPS requested some additional information from the Parliament by letter of 26 May 2021. The Parliament provided its reply with two letters, on 8 and 17 June 2021, respectively.

On 14 April 2021 noyb filed a request for access to the file under Article 41(2)(b) of the EU Charter of Fundamental rights. The EDPS replied on 5 May, 20 July and 7 December 2021, respectively.

PART II - Facts

In order to provide MEPs and the Parliament's staff with the possibility to be efficiently and swiftly tested in the context of the COVID-19 pandemic, the Parliament contracted the private company Ecolog to conduct mass COVID-19 PCR testing within the Parliament's premises and run the europarl.ecocare.center website. In order to respect the epidemiological precautions, testing is conducted following online registration. The dedicated website went online on 30 September 2020.

The complainants used the software *webbkoll* from the Danish non-profit organisation *Dataskydd* to scan the dedicated website and identify cookies and trackers that the website used. The complainants became aware of the existence of Google analytics and Stripe cookies on the dedicated website through the webbkoll report. They used the report produced by webbkoll as a basis for their allegations as summarised below.

On 27 October 2020, one of the complainants sent an email to the Parliament's Secretariat and all MEPs informing them of the webbkoll technical analysis of the website and inquiring about the justification for the transfers of MEPs' and staff's personal data to the US.

In addition, on 29 October 2020, the complainants filed a complaint with the Parliament's DPO. The DPO acknowledged receipt of the complaint on the same day. On 13 November 2020, the Parliament's DPO informed the complainants that 'new internal technical verifications on the web page of the test centre confirmed that it is currently not possible to transfer any data to third countries'. He additionally informed the complainants that 'further analysis is ongoing in order to verify the data workflow in the first period of activity of the centre and determine whether transfers to third parties did actually happen'.

On 18 November 2020, the Parliament's Secretariat replied to the complainants' email of 27 October 2020, informing them that its Directorate-General for Personnel ('DG PERS') is the controller for the processing of personal data on the website and that Regulation (EU) 2018/1725 is applicable. The Secretariat further informed that 'DG PERS has received assurances from Ecolog and has since verified that Google analytics and Stripe have been disabled on the registration platform'.

Following receipt of the Secretariat's email, the complainants sent on 1 December 2020 an email to the Parliament's Secretariat and the Parliament's DPO respectively, inquiring 'how long exactly did the data transfers happen via Google Analytics and Stripe cookies', as well as 'what kind of data from MEPs, APAs [Accredited Parliamentary Assistants] and employees were transferred'.

On 7 December 2020, the complainants received a reply from DG PERS,[2] which explained that 'they established that one cookie and several tracks to servers (sic) located in Germany, Finland and USA were present on the webpage at issue. As [the complainants] referenced in [their] email of 1 December 2020, the trackers from Google analytics and Stripe were disabled by Ecolog in the days following [the] complaint. Subsequently, Ecolog confirmed that no data transfers had taken place in the context of the cookie and trackers at issue'. In the same email, DG PERS stated that they requested Ecolog to provide them with 'detailed explanations' in order to ensure that 'no data transfers had occurred before the removal of the trackers from Google analytics and Stripe'. They further explained that 'the company confirmed that the Stripe cookie (for secure payments) in the webpage had never been active, since registration for testing for EU Staff and Members did not require any form of payment. Further, the trackers were used only to ensure that the application was called only from the domain ecolog-international.com (domain of the company)'. DG PERS also informed the complainants that no personal data of MEPs and the Parliament's staff, registered for COVID-19 testing through the website, were transferred outside the EU.

On 16 February 2021, the EDPS informed the Parliament, through his letter inviting its comments on the complaint, of the fact that the complainants' request of 27 October 2020 to be informed of the transfers of their personal data and the appropriate safeguards for such transfers constitutes a request for access to personal data under Article 17 of the Regulation. He further inquired how the Parliament had handled or planned to handle the request.

By letter of 25 March 2021, the Parliament informed the EDPS that it was in no position to identify neither the users of the website (or IP addresses of users), who accepted the Google Analytics cookies on the website, nor the personal data that were sent to Google from the use of such cookies. In the same letter, however, the Parliament admitted that 'Ecolog did not provide the EP services with complete certainty regarding the absence of data transfers to the US'.

[2] A copy of this email was transmitted on 17 December 2020 to the EDPS by the Parliament's DPO.

Allegations of the complainants

1. The Parliament's website and alleged transfers to the United States (US)

On the basis of the aforementioned webbkoll report, the complainants alleged that the dedicated website incorporated (at the time of the initial complaint) 'a third party cookie and a total of 150 third-party requests', among which 'several trackers', including one that belonged to a company located in the US.

The complainants claimed that the findings in the webbkoll report were an indication that the Parliament was transferring personal data relating to MEPs and employees outside the European Union, in particular to Google and Stripe in the US. In their view, such a transfer of personal data is contrary to the recent Schrems II judgment of the Court of Justice of the European Union.[3] Regarding transfers to Google, the complainants put forward that this is confirmed by the data protection notice on the website,[4] which stated, at least until the '13 January 2021',[5] that 'the information regarding [the] usage of this website generated by the use of Google Analytics is transmitted to and stored on a Google server in the US'.

In light of the findings of the webbkoll report and the information included in the website's data protection notice, the complainants contested the information provided by DG PERS.

2. Data protection notice on the Parliament's website

The complainants alleged that at least until '13 January 2021', visitors to the website were presented with two different data protection notices:[6] one under the 'data protection' section at the bottom of the homepage,[7] and one on the registration page of the website.[8] The complainants noted that both data protection notices failed to refer to Regulation (EU) 2018/1725. Furthermore, the complainants observed that the notices referred instead to the GDPR and in particular mention legitimate interest under Article 6(1)(f) GDPR as the legal basis for the processing. They pointed out that this provision does not have any equivalent under the Regulation. In the complainants' view, the above elements constitute violations of Articles 5, 14 and 15 of the Regulation.

3. Cookie banner on the Parliament's website

In addition, the complainants pointed out that at the time of the filing of the complaint, visitors to the website were presented with a different cookie banner depending on the language setting of the website. In particular, the English version of the banner only displayed an 'essential' tick box, whereas the French and German versions additionally

[3] Judgment of the Court of Justice of 16 July 2020 in case C-311/18, *Data Protection Commissioner v. Facebook Ireland LTD and Maximillian Schrems* ("Schrems II"), EU:C:2020:559.
[4] https://europarl.ecocare.center/.
[5] According to checks carried out by the EDPS, the data protection notice was online at least until 1 February 2021.
[6] According to checks carried out by the EDPS, the two data protection notices were online until 1 February 2021.
[7] https://europarl.ecocare.center/.
[8] https://europarl.ecocare.center/registration/.

included an 'external media' tick box. The German cookie banner also included the option to 'accept only necessary cookies', an option absent from the English and French versions. Clicking the 'cookie details' section of the banners would take visitors to the second layer of the cookie banners, which were again different depending on the language displayed. The English version only referred to essential cookies and prompted the user to either click on the 'accept all' or the 'save' button. The difference between the two buttons was unclear. The French version of the second layer of cookie banner referred both to essential cookies and 'external media'. These external media cookies included cookies from Facebook, Google Maps, Instagram, OpenStreetMap, Twitter, Vimeo and Youtube. The visitor could also choose between 'accept all' or 'save'. The German version of the second layer of the cookie banner referred to only one 'external media' cookie - Google Maps - in addition to the essential cookie.

The description of the essential cookie provided in all three banners stated that it 'saves the visitors' preferences selected in the Cookie Box of Borlabs Cookie'. The complainants claimed that information relating to the essential cookie was not 'clear, concise and intelligible', 'especially when it comes to the banner of the English version, where no preference regarding cookies can be selected by the users', which constitutes a violation of Article 14 of the Regulation.

Furthermore, the complainants claimed that there was no 'reject all' option on the first layer of the cookie banner, which constitutes a violation of Article 14 of the Regulation, as well as non-compliance with the conditions set out in the Regulation for valid consent.

The complainants additionally alleged that the design of the cookie banners was deceptive, since they prompted the website's visitors to 'accept all' cookies, by highlighting the corresponding button. They also added that there was no information about the withdrawal of consent for the use of cookies on the website.

4. Access to personal data request

Finally, the complainants requested that their right of access to their personal data under Article 17 of the Regulation be satisfied. In particular, they requested to be 'informed of which of their data exactly were transferred abroad' and to be 'made aware of what appropriate safeguards and additional measures are put in place for the transfer' outside of the EU.

Comments of the data controller

1. On Google Analytics, the Stripe cookie, any additional trackers on the website and transfers of personal data to the US

Due to the fact that the website was set up by Ecolog as a 'sub-site' of Ecolog's main website, the latter offering testing services to clients other than the Parliament for which payment is required, the Stripe cookie remained available on the Parliament's dedicated website for the period between 30 September to 2 November 2020, when it was removed by Ecolog under the Parliament's instructions. However, 'Stripe cookies are used only when [a] person is redirected to do online payment via this service. As online payment was not an option in

[the] European Parliament app it was never active and nothing is transferred (sic)'. According to the Parliament, this explains the contradiction between the findings of the webbkoll report submitted by the complainants and the Parliament's explanation regarding the said cookie not being active. In fact, the Parliament's website, set up by Ecolog, 'contained some parts of code copied from another webpage that the company built for a test centre in the Brussels International Airport (Zaventem). The parts copied included the code for a cookie from Stripe that was used for online payment for users in Zaventem. The page for European Parliament tests was not directing any user to the online payments module as no payment is required for testing in the European Parliament. For this reason, the analysis shows the presence of code for Stripe but it was not actually used'.

The Parliament claimed that 'unfortunately, and without any instruction given by the European Parliament in this regard, Google cookies were present and active on the website from September 30th to November 4th, 2020'. According to Ecolog's information to the Parliament, these cookies were used in order to minimise the risk of spoofing and for website optimisation purposes. Following the Parliament's instructions in early November, all cookies except an 'internal' one used by the website were removed. The internal cookie was removed in February 2021.

According to Google's terms of use, Google Analytics are designed to process 'online identifiers, including cookie identifiers, internet protocol addresses and device identifiers' as well as 'client identifiers'. The Parliament explained that users connecting through the Parliament's network use 'an anonymised IP address' and that 'possible transfers of information could occur only in cases where users connected to the webpage from private connections outside the network of the EP, accepted the cookies from the website and did not have cookies disabled in their browsers'.

The Parliament further admitted that Ecolog's explanation on the absence of personal data transfers to the US did not provide 'complete certainty' that no such transfers had taken place; 'on the contrary, it is reasonable to state that, only during the mentioned period of October 2020, a transfer of data was possible'. However, the Parliament pointed out that the risk for data subjects concerned was low, taking into account the types of personal data processed and the amount of users affected '(only end-users connecting to the web from private connections)'.

2. <u>On the data protection notice on the Parliament's website and the cookie banner</u>

According to the controller, the website featured two different data protection notices, at the time of the complaint. The one at the main entry page was copied from the Zaventem page and the one on the registration page was slightly different, but the Parliament acknowledged that neither was 'appropriate', as they 'contained wrong and misleading information'.

Following receipt of the complaint, the Parliament focused on 'removing the cookies', 'publishing the right Privacy Statement' and 'removing misleading information from the cookies preferences box'. The Parliament provided Ecolog with the updated English version of the data protection notice on 3 February 2021. The French and German versions were published on the relevant website on 24 February 2021. The Parliament provided the EDPS

with links to the updated versions of the data protection notices, as well as screenshots of the online registration form.

3. On the request of access to personal data

Following the EDPS' request for comments, the Parliament claimed that it was in no position to identify neither the users (or IP addresses of users), who accepted the Google Analytics cookies on the website, nor the personal data that were sent to Google because of the use of such cookies. However, its assessment suggested that 'the volume of possibly impacted data subjects remains limited', 'having in mind the fact that only end-users connecting to the web from private connections and accepting the presented cookies policy might be subject to data transfers'. The Parliament believes that this claim is further supported by 'the consideration that the European Parliament equipped Parliament members and staff members with devices allowing them to use the EP internal secured working platform for making appointments'.

PART III - Legal analysis

1. Data controllership

In the context of the investigation, the EDPS requested the Parliament to provide information revealing its contractual relationship with Ecolog, as well as Ecolog's discretion, and limits thereof, in the setting up and functioning of the Parliament's dedicated website.

Within this framework, the Parliament provided its contract with Ecolog and email correspondence between them that took place during the period between 25 January and 19 March 2021 (relevant correspondence).

Article 3(8) of the Regulation defines the controller as the entity that determines[9] the purposes and the means[10] of the processing. In identifying a controller, questions such as 'why the processing is taking place', 'who initiated the processing' and 'who benefits from the processing', as well as 'how the processing is taking place' are essential. Whereas it is the controller who determines the 'essential' elements of the means of the processing, such as the type(s) of data to be processed, the period for which they would be retained, from which data subjects the data would be collected, etc., more practical aspects of the processing, such as the software or the technical security measures, can be determined by the data processor, to the extent that such operation is being undertaken under the general instructions of the data controller.[11] In fact, the processor may enjoy a considerable degree of autonomy in providing its services and may identify the 'non-essential' elements of the processing operation.[12] The processor may advise or propose certain measures in this respect, but it is up to the controller to decide whether to accept such advice or proposal, after having

[9] See EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 (EDPS Guidelines on controllership), section 3.1.2, available at https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.
[10] See EDPS Guidelines on controllership, section 3.1.3.
[11] See EDPS Guidelines on controllership, section 3.1.3.
[12] See EDPS Guidelines on controllership, section 4.1.2.

been fully informed of the reasons for the measures, what the measures are and how they would be implemented.[13]

The contract concluded on the Parliament's own initiative with Ecolog sets out the conditions under which Ecolog should establish a provisional COVID-19 testing centre on the premises of the Parliament in Brussels through an integrated solution and provide its services accordingly. Testing services based on the contract were to be made available to MEPs and other staff of the Parliament. The contract states that the controller of the processing operation is the Brussels Medical Service of the Parliament. The contract further lists the types of personal data to be processed, the operations that the processing comprises as well as the purpose of the processing, which is the recording and classification of any information relating to the performance of the COVID-19 tests. Whereas the contractual arrangements reveal the Parliament's intention to be the controller for the processing operations that fall within the contract framework, the EDPS still needed to assess the level of instructions the Parliament gave to Ecolog in this regard, in order to determine whether the Parliament is indeed the sole controller and exclude a case of joint controllership.

It follows from the relevant correspondence between Ecolog and the Parliament that the latter delegated the setting up and functioning of the website to Ecolog. The correspondence reveals that before setting up the website, Ecolog had consulted the Parliament about the 'complete website and the privacy statement (including the use of cookies)', which were approved by the Parliament. Therefore, Ecolog was 'under the assumption that the technical set-up' was 'in line with [the Parliament's] regulations'. Furthermore, 'in the beginning of [their] cooperation [with the Parliament]', Ecolog made the Parliament 'aware that the privacy statement should have come from the Parliament and not from [them], as [they are] only the data processor and not the data controller according to the contract'. Ecolog drafted the data protection notice 'only as courtesy and in order to [provide] support on short notice'.

Based on the above, the EDPS considers the Parliament as the sole data controller for the processing in question, i.e. the operation of the Parliament's dedicated website, whereas Ecolog acts as a processor.

According to Article 26(1) of the Regulation, '(...) the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'. Article 26(2) of the Regulation provides that 'where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller'.

According to Article 29(1) of the Regulation, 'the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures' in order to ensure respect of the requirements of the Regulation and the rights of the data subject. The controller is therefore responsible for assessing the guarantees provided by the processor and should be able to demonstrate that it has taken into account all requirements of the Regulation. In practice, the processor should demonstrate to the satisfaction of the controller such guarantees, which implies an exchange of relevant

[13] See EDPS Guidelines on controllership, section 4.1.2.

documentation (e.g. data protection notice, information security policy etc.). Assessing the processor's guarantees is done on a case-by-case basis, taking into consideration the nature, the scope and the purposes of the processing, as well as the risks to the rights and freedoms of the data subjects. In any case, one of the elements that the controller should also evaluate is the processor's expert knowledge.[14]

Article 29(3) of the Regulation requires that 'any processing by a processor shall be governed by a contract or other legal act under Union or Member State law' between the controller and the processor. In accordance with Article 29(9) of the Regulation, such a contract or legal act must be in writing, and should contain all elements listed under Article 29(3) of the Regulation, as well as detailed instructions on how these elements must be implemented.[15] Such instructions can outline, among others, permissible or unacceptable handling of personal data, and they must be documented. Whereas it is recommended that such instructions are annexed to the contract or legal act, instructions in other forms (e.g. by email) are also acceptable, provided that it is possible to keep record of them.[16]

Both the controller and the processor are responsible for ensuring that a contract or legal act, in line with Article 29(3) of the Regulation, is in place.

The Parliament delegated the setting up and functioning of the website to Ecolog.[17] Ecolog informed the Parliament that the use of the Google Analytics cookies aimed to optimise the website and minimise the risk of spoofing. Determining the use of cookies for the Parliament's dedicated website is an action that Ecolog carried out while operating under the Parliament's general instructions (i.e. the setting up and functioning of the website) in this regard.

Ecolog's use of the Stripe cookies seems to be the result of human error while setting up the Parliament's dedicated website. When creating the Parliament's website, Ecolog copied the code of another website that it had previously built for a different client, which required online payment carried out through the Stripe cookies.

By assigning Ecolog to set up and ensure the functioning of the dedicated website, as well as to draft the data protection notice, the Parliament, as the controller for the processing operation in question, seems to have chosen to give operational independence and discretion to Ecolog, the processor. The Parliament did so while being aware that such tasks are not within Ecolog's primary field of expertise and knowledge (this being rather the provision of COVID-19 testing services) and without having any sufficient guarantees by Ecolog that it could implement appropriate technical and organisational measures to carry out these tasks in line with the Regulation. The Parliament's claim that the Google Analytics cookies were used on the website 'without any instruction given by the European Parliament in this regard' does not change the fact that the primary duty of compliance lies with the

[14] See EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (EDPB Guidelines on controllership), paragraphs 95-97, available at https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.
[15] EDPB Guidelines on controllership, paragraph 112.
[16] EDPB Guidelines on controllership, paragraph 118.
[17] Information derived from the relevant correspondence, quoted earlier in the text.

controller.[18] Furthermore, the Parliament approved the work done by Ecolog in this context, before the dedicated website went public. In doing so, the Parliament did not show the necessary diligence required from a data controller and, ultimately, failed to comply with the Regulation, in particular with Articles 26(1) and 29(1) of the Regulation.

Finally, based on the evidence submitted to him, the EDPS considers that the Parliament failed to provide the necessary detailed instructions to Ecolog for the setting up of the website, including the drafting of the data protection notice. Since the Regulation establishes a clear obligation, where no other relevant legal act is in force, for the written contract to stipulate that the personal data must be processed only on documented instructions from the controller the absence thereof is an infringement of Article 29(3) of the Regulation.

2. Transparency and information requirements

Article 4(1)(a) of the Regulation establishes the principles of lawfulness, fairness and transparency that apply to all personal data processing operations. The principle of transparency establishes an obligation for the controller to take all appropriate measures in order to keep the data subjects informed about the processing of their personal data. Transparency may refer to the information given to data subjects before the processing starts or to the information that should be easily accessible to them during the processing.

The accountability principle, established in Article 4(2) of the Regulation, requires controllers to actively and continuously implement measures to promote and safeguard data protection in their processing activities.[19] Controllers shall ensure, verify and be able to actively demonstrate compliance with the provisions of the Regulation, both to the data subjects and to their supervisory data protection authority, at any time.

Article 14 of the Regulation imposes the obligation on the controller to provide data subjects with information regarding the processing of their personal data in a transparent and easily accessible form. This information should be presented in a clear and plain language before the processing starts. The Regulation's transparency and information requirements can be met through a specific data protection notice. The information included in the data protection notice should be in line with Articles 15 and, where applicable, 16 of the Regulation.

The Parliament updated all three linguistic versions of the data protection notices on the main page and the registration page of the website in February 2021. As submitted by the complainants and the Parliament, as well as verified by the EDPS's assessment, the previous versions of these notices did not reflect the processing done by the Parliament, since they were data protection notices copied from the testing center of Zaventem's airport and, consequently, did not meet the requirements of transparency of the Regulation. The mention of the legal base for processing as being Article 6(1)(f) GDPR, stems from the above error consisting in carrying over a data protection notice conceived for a different situation.

[18] See EDPS Guidelines on controllership, section 4.1.2 and Article 4(2) of the Regulation.
[19] See also Article 26 of the Regulation.

Based on the above, the EDPS considers that until February 2021, by failing to provide accurate data protection notices on the website, the Parliament contravened its obligations under Articles 4(1)(a) and 14 (principle of transparency), Article 4(2) (accountability principle), and Article 15 (data subject's right to information) of the Regulation.

Whereas the updated versions of the notices are indeed improved compared to the previous ones, the EDPS would like to highlight that further changes are still required in order to meet the transparency and information requirements of the Regulation.

In particular, the data protection notices state that 'Articles 15 and 16 of [the] Regulation (…) apply to the processing of personal data carried out by the European Parliament'. This statement is misleading, as the Regulation applies in its entirety; Articles 15 and 16 define which information should be provided to data subjects in the context of the processing of their personal data, through a data protection notice. In addition, Article 16 of the Regulation only applies in cases where personal data have not been obtained from the data subject, which does not seem to be the case for the processing at hand.

Furthermore, the list of personal data processed contains reference to the 'symptoms' and 'results of COVID-19 test'. Such data are data concerning health within the meaning of Article 3(19) of the Regulation, revealing information about the health status of a data subject. Such a processing should be reflected under the section on the legal grounds for the processing. Based on the information received (screenshot of the online registration form), as well as the EDPS' assessment, the Parliament does not process data concerning health in the context of the functioning of the website. The actual processing should be reflected in the data protection notice, which should be further updated accordingly. In case the Parliament's practice has changed in the meantime and processing of data concerning health does indeed take place, the Parliament should additionally include a reference to Article 10 and the relevant legal ground(s) for such processing.

The data protection notices do not explicitly mention the duration of the data retention period, but state that the personal data 'will be kept by the [processor] and the controller until the end of the provision of services relating to processing, as stated in the contract'. They also mention that 'data related to the test result will be stored in [the] medical file in accordance with the retention period applicable to those files'.

In accordance with Article 15(2)(a) of the Regulation, the period for which the personal data will be stored or, in case this is not possible, the criteria used to determine that period, should be mentioned in the data protection notice. For transparency purposes and for easy access to this information, the data protection notices on the dedicated website should be updated to reflect the already determined retention period of the medical files, in which data relating to the test results are stored. For the same reasons, the Parliament should define how long the processor should keep the data or at least explain the factors that are taken into account to determine this retention period. In doing so, it should take into account the principle of storage limitation of Article 4(1)(e) of the Regulation, according to which it must be ensured that the period for which personal data are stored is limited to what is necessary for the purpose of the processing. To this end, the data controller should establish time limits for

erasure or for periodic review.[20] In this context, it is worth highlighting that storing data 'until the end of the provision of services', based on a contract, is not in line with the principle of storage limitation, because there is no link between the storage of the data and the provision of the services, which is undetermined time-wise.

The sections of the data protection notices relating to the recipients of the personal data fail to make any reference to the processor. According to Article 3(13) of the Regulation, recipients are any natural or legal person, public authority, agency or another body, to which personal data are disclosed. Recipients can either be distinct from the controller or processor or belong to the controller or processor, such as an employee or another division within the same company or authority. Since, according to the data protection notices, the processors are consulting, transmitting and storing personal data, the Parliament should list the processors under the recipients.[21]

The EDPS observes a remaining inconsistency between the different linguistic versions of the data protection notices. The English and German versions refer to Ecolog and the Laboratory van Poucke as processors under Article 29 of the Regulation, whereas the French version refers to them as controllers ('responsables du traitement'). Finally, the DPO's contact details on the website refer to Ecolog, in all three linguistic versions of the website, when they should be referring to the Parliament.[22]

Based on the above, the EDPS considers that, as at the date of the present decision, the Parliament remains not fully compliant with Articles 4(1)(a) and 14 (principle of transparency), Article 4(2) (accountability principle), and Article 15 (data subject's right to information) of the Regulation.

3. Cookies and transfers of personal data to the US

Cookies 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 within their own web service or with others using those cookies. Cookies are used, among others, to enable user authentication during sessions and to contribute to web service improvement, by recording browsing behaviour.[23]

Article 3(1) of the Regulation defines personal data as any information relating to an identified or identifiable natural person. In this context, identifiable natural person refers to a person who can be identified, directly or indirectly, by reference, among others, to an identifier, such as name, identification number, or an online identifier. According to Recital 18 of the Regulation, natural persons may be associated with online identifiers provided by their devices, applications and protocols, such as internet protocol addresses (IP addresses), cookie identifiers or other identifiers. This information can lead to the identification of the

[20] See Recital 20 of Regulation (EU) 2018/1725.
[21] See Article 29 Working Party Guidelines on transparency under Regulation 2016/679, Annex, page 37.
[22] See https://europarl.ecocare.center/dpo/, https://europarl.ecocare.center/fr/dpo/ and https://europarl.ecocare.center/de/dpo/.
[23] See EDPS Guidelines on the protection of personal data processed through web services provided by EU institutions, paragraph 22 (EDPS Guidelines on web services), available at https://edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_web_services_en.pdf.

natural persons, in particular when combined with unique identifiers and other information received by the servers. Any processing of personal data done by EU institutions, bodies and agencies (EUIs), including through cookies, is covered by the Regulation.[24]

Tracking cookies, such as the Stripe and the Google analytics cookies, are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection.[25] All records containing identifiers that can be used to single out users, are considered as personal data under the Regulation and must be treated and protected as such.[26]

Upon installation on the device, a cookie cannot be considered 'inactive'. Every time a user visited Ecolog's website, personal data was transferred to Stripe through the Stripe cookie, which contained an identifier. Neither the Parliament nor Ecolog have argued that there were any technical measures in place to prevent such transfers. Whether Stripe further processed the data transferred through the cookie is not relevant.

Google Analytics cookies, which the Parliament acknowledged were present on the website, are designed to process 'online identifiers, including cookie identifiers, internet protocol addresses and device identifiers' as well as 'client identifiers', according to the controller.

Therefore, the EDPS considers that personal data of visitors to the Parliament's dedicated website were processed through the abovementioned trackers even if this only happened where users visited the website through a network other than the Parliament's. For the period between 30 September and 4 November 2020, during which the trackers remained on the website, personal data processed through them were transferred to the US, where both

Stripe and Google LLC are located. The conclusion that transfers to the US took place is reinforced by the circumstance highlighted by the complainants, according to which, 'all data collected through Google Analytics is hosted (i.e. stored and further processed) in the USA'.[27] Furthermore, the first version of the Parliament's data protection notice on the dedicated website referred to the use of Standard Contractual Clauses (SCCs) for the transfers of data outside of the EU, which is what Google refers to in its data protection notice in order to inform of transfers of data from the EU/EEA to non-EU/EEA countries.

The EUIs must remain in control and take informed decisions when selecting processors and allowing transfers of personal data outside the EEA.[28] The EDPS recalls that absent an adequacy decision for transfers to, among other destinations, the US, controllers and processors may transfer personal data to a third country only if appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies

[24] See EDPS Guidelines on web services, paragraph 92
[25] See EDPS Guidelines on web services, paragraph 94.
[26] See EDPS Guidelines on web services, executive summary.
[27] See Google's reply No 8 in its answers to the Austrian Supervisory Authority (Österreichische Datenschutzbehörde) regarding the use of Google Analytics in the context of the 101 complaints filed by noyb on the transfer of data to the US when using Google Analytics.
[28] See EDPS strategy for Union institutions, officers, bodies and agencies to comply with the 'Schrems II' ruling, section 2, available at https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

for data subjects are available[29]. Such safeguards may be provided in Standard Contractual Clauses (SCCs) or another transfer tool. The transfer tool relied on must ensure that data subjects, whose personal data are transferred to a third country pursuant to that transfer tool, are afforded a level of protection in that third country that is essentially equivalent to that guaranteed within the EU by EU data protection law, read in the light of the Charter[30].

However, the use of SCCs or another transfer tool (e.g. *ad hoc* contractual clauses) does not substitute the individual case-by-case assessment that an EUI as a controller must carry out, in accordance with the *Schrems II* judgement, to determine whether in the context of the specific transfer, the third country of destination affords the transferred data an essentially equivalent level of protection to that in the EU. The EUI, where appropriate in collaboration with the data importer in the third country, must carry out this assessment of the effectiveness of the proposed safeguards before any transfer is made or a suspended transfer is resumed.

Where the essentially equivalent level of protection for the transferred data is not effectively ensured, because the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the used SCCs for transfers or another transfer tool, the EUI must implement contractual, technical and organisational measures to effectively supplement the safeguards in the transfer tool, where necessary together with the data importer[31].

In the Schrems II judgement, the Court of Justice found that the level of protection of personal data in the US was problematic in view of the lack of proportionality caused by mass surveillance programmes based on Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333 read in conjunction with Presidential Policy Directive 28[32] and the lack of effective remedies in the US essentially equivalent to those required by Article 47 of the Charter.[33] Following this, the EDPS is of the view that transfers of personal data to the US can only take place if they are framed by effective supplementary measures in order to ensure an essentially equivalent level of protection for the personal data transferred.

However, the Parliament provided no documentation, evidence or other information regarding the contractual, technical or organisational measures in place to ensure an essentially equivalent level of protection to the personal data transferred to the US in the context of the use of cookies on the website. The EDPS therefore considers that the Parliament failed to meet the requirements of Article 46 and Article 48(2)(b) of the Regulation for the period between 30 September and 4 November 2020, during which the cookies in question were present on the dedicated website.

[29] Article 48(1) of the Regulation.
[30] See Article 46 and recitals (65) and (70) of the Regulation, as well as paragraphs 96 and 103 of the Schrems II judgement.
[31] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0 Adopted on 18 June 2021.
[32] Points 179 to 185 of the *Schrems II* judgement.
[33] Points 186 to 199 of the *Schrems II* judgement.

4. Cookie banner on the Parliament's dedicated website

In line with Articles 26(1) and 37 of the Regulation, the controller must implement appropriate technical and organisational measures to ensure the protection of information transmitted to, stored in, related to, processed by and collected from the user's terminal equipment when accessing the EUI's publicly available website, in accordance with Article 5(3) of Directive 2002/58/EC (ePrivacy Directive).[34] The controller should be able to demonstrate that the processing is performed in accordance with the Regulation.

According to Article 5(3) of the ePrivacy Directive, 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,[35] inter alia, about the purposes of the processing'. 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'. Article 5(3) applies to any information stored in such terminal equipment, regardless of whether or not it is personal data.[36]

Therefore, before setting cookies or any other technology falling within the scope of Article 5(3) of the ePrivacy Directive, the EUI must provide the user with adequate information on what is accessed or stored on the user's terminal equipment, on the purposes of this action and the means for expressing their consent. No action may be performed before the consent is collected. In addition, users must be enabled to withdraw their consent at any time.[37]

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.[38] Generally, the EUIs' web services should be able to work without cookies requiring consent.[39]

Tracking cookies from social plug-ins, third-party advertising and analytics clearly require the data subject's consent. Even first-party analytics, which 'are often considered as a "strictly necessary" tool for web service operators, are not strictly necessary to provide a functionality explicitly requested by the user and are consequently, in principle, subject to the requirement of consent.[40]

[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 , 31.07.2002, p. 0037 - 0047.
[35] Directive 95/46/EC is repealed with effect from 25 May 2018. References to the repealed Directive shall be construed as references to the General Data Protection Regulation, the mirror Regulation of Regulation (EU) 2018/1725.
[36] CJEU, C-673/17, *Planet 49*, paragraphs 70-71.
[37] See EDPS Guidelines on web services, paragraph 26.
[38] See EDPS Guidelines on web services, paragraph 26.
[39] See EDPS Guidelines on web services, executive summary.
[40] See EDPS Guidelines on web services, paragraph 103.

Based on the aforementioned, the Parliament's cookie banner text should refer to the types of information accessed or stored through the cookies as well as the purposes for such access or storage, and the information conveyed through the banner should be identical in all linguistic versions. Finally, it should provide users the option to consent or not to the processing of non-essential cookies. In this regard, the banners should include an opt-in button allowing users to accept cookies, making it clear that by clicking on the button users agree to the deployment of cookies. Such button should not be preselected; users must not need to intervene in order to prevent agreement with the processing.[41] So called 'cookie walls' are not in line with the Regulation, meaning that for consent to be freely given, access to the website's service and functionalities should not depend on the users' consent for cookies that are not strictly necessary in the sense described above. Finally, in case personal data collected through the cookies are shared with third parties, such as analytics partners, the cookie banner should draw the users' attention to it.

The complainants' allegations regarding the cookie banner, as presented under number 3 of the 'Allegations of the complainants' section of the present decision, were verified by the EDPS. Indeed, from the publication of the dedicated website to at least February 2021, the Parliament's cookie banners differed depending on the linguistic version. With regard to the complainants' claims under points 69 (10) to (14) of the complaint, the EDPS has reached the conclusion that the cookie banners in all three languages were not in line with the definition of consent under Article 3(15) of the Regulation nor did they meet the requirements of Article 37 of the Regulation and Article 5(3) of the ePrivacy Directive, as described above. The cookie banner further failed to provide transparent information regarding the processing of personal data in relation to the cookies on the website, which constitutes the Parliament's infringement of Article 14(1) of the Regulation, as elaborated in section 2 of the legal analysis of the present decision.

5. Request for access to personal data

The EDPS considers the complainants' request to be informed of which data were transferred through Google Analytics and Stripe to the US, as well as the appropriate safeguards for such transfers, as a request for access to personal data under Article 17 of the Regulation.

Article 17(1) of the Regulation provides the right of data subjects to obtain from the controller confirmation as to whether or not personal data concerning them are being processed and, if answered in the affirmative, to access these personal data (...). In accordance with Article 14(3) of the Regulation, the controller must reply to a request for access without undue delay and in any event within one month of receipt of the request. Article 14(4) of the Regulation provides that in case the controller does not take action on the request of the data subject, the data subject must be informed without undue delay, and, at the latest, within one month of receipt of the request of the reasons for not taking action, as well as on the possibility for lodging a complaint with the EDPS and seeking judicial remedy.

The complainants contacted the Parliament and its DPO late October 2020, inquiring about the justification for transfers of MEPs' and staff's personal data to the US. The Parliament

[41] See EDPB Guidelines 05/2020 on consent under Regulation 2016/697, paragraph 81, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

replied on 7 December 2020, explaining that they had 'established that one cookie and several tracks to servers (sic) located in Germany, Finland and USA were present on the webpage at issue. (...) [T]he trackers from Google analytics and Stripe were disabled by Ecolog in the days following [the] complaint. Subsequently, Ecolog confirmed that no data transfers had taken place in the context of the cookie and trackers at issue'.

On 16 February 2021, the EDPS informed the Parliament, through his letter inviting its comments on the complaint, of the fact that the complainants' request to be informed of the transfers of their personal data and the appropriate safeguards for such transfers constitutes a request for access to personal data under Article 17 of the Regulation. He further inquired how the Parliament had handled or planned to handle the request. By letter of 25 March 2021, the Parliament informed the EDPS that it was in no position to identify neither the users (or IP addresses of users), who accepted the Google Analytics cookies on the website, nor the personal data that were sent to Google from the use of such cookies. The Parliament did not make any reference to the Stripe cookie. In the same letter, however, the Parliament admitted that Ecolog's explanation on the absence of personal data transfers to the US through cookies did not provide 'complete certainty' that no such transfers had taken place; 'on the contrary, it is reasonable to state that, only during the mentioned period of October 2020, a transfer of data was possible'.

It therefore becomes apparent that, at least in March 2021, the Parliament was aware that the complainants' personal data had been processed through the cookies, which were present on the website for the period between 30 September to 4 November 2020, since transfers of personal data had taken place. Consequently, and especially following the EDPS' inquiry on the matter, the Parliament should have replied to the complainants' access to personal data request.

In particular, in line with Article 17(1) of the Regulation, the Parliament should have provided the complainants with confirmation as to the fact that their personal data had been processed in the context of the use of third party cookies on the Parliament's dedicated website. Had it subsequently demonstrated the impossibility to identify the data subjects, the Parliament should have informed them accordingly, in line with Article 14(4) of the Regulation.

The Parliament should have provided the relevant information even if it was aware that the processing of the personal data in question was unlawful, as the main purpose of the right of access under Article 17 is precisely to enable data subjects to become aware of the processing and verify the lawfulness thereof, or exercise other data subject rights.[42]

Therefore, the EDPS considers that the Parliament failed to meet its obligations under Articles 17 and 14(4) of the Regulation.

[42] See also *C-553/07* Rijkeboer, ECLI:EU:C:2009:293, in particular paragraphs 49 and 51.

6. Use of corrective power under Article 58(2)(i) and 66 of the Regulation

The complainants request that the EDPS make use of his corrective power under Article 58(2)(i) of the Regulation. This provision states that the EDPS has the power to issue an administrative fine pursuant to Article 66 in case an EU institution fails to comply with one of the corrective measures of Article 58(2)(d) to (h) and (j) of the Regulation. The conditions of the Regulation for the imposition on an administrative fine are not met because the EDPS is not making use of those types of corrective measures. Therefore, the EDPS is not imposing an administrative fine to the Parliament.

PART IV- Conclusion

In light of the above, the EDPS concludes that the Parliament has infringed the following Articles of the Regulation:

a. Articles 26(1) and 29(1) due to its failure to fulfil its responsibilities as controller and use a processor providing sufficient guarantees to implement appropriate technical and organisational measures;
b. Article 29(3) due to its failure to provide documentation relating to the detailed instructions given to the processor for the setting up and functioning of the website;
c. Articles 4(1)(a) and 14, 4(2), and 15 due to its failure to respect the principle of transparency, accountability and the data subjects' right to information because of the inaccurate data protection notice and cookie banner on the dedicated website;
d. Article 46 and Article 48(2)(b) of the Regulation, due to its reliance on the Standard Contractual Clauses in the absence of a demonstration that data subjects' personal data transferred to the US were provided an essential equivalent level of protection;
e. Article 37 read in the light of Article 5(3) of the ePrivacy Directive, due to its failure to protect information (the cookies) transmitted to, stored in, related to, processed by and collected from the users' terminal equipment;
f. Articles 17 and 14(4) due to its failure to reply to the data subjects' request for access to their personal data.

On the basis of the facts and findings as described above, the EDPS decides:

1. to issue a reprimand to the Parliament in accordance with Article 58(2)(b) of the Regulation, for the above infringements;

2. to order the Parliament, pursuant to Article 58(2)(b) of the Regulation, to update its data protection notices in the dedicated website in order to provide all relevant information relating to the processing of personal data. The Parliament should address this order **within one (1) month from the date of this decision**.

In determining the corrective powers used in the present case, the EDPS takes into account the possibly large number of data subjects affected by the Parliament's abovementioned infringements and the impact these had on the former's fundamental rights and freedoms, as well as the duration of said infringements.

The EDPS notes that the Parliament has been consistently responsive and collaborative throughout the investigation of the complaint, and that as at the date of the decision most of the infringements have been remedied.

Pursuant to Article 59 of the Regulation, the Parliament must inform the EDPS, **within three months since the date of this decision,** of its views in relation to the abovementioned reprimand.

Done in Brussels, 5 January 2022

[e-signed]

Wojciech Rafał WIEWIÓROWSKI