31 May 2024

Secretariat Unit 01
European Commission
DG Justice and Consumers
Unit 01 – International Affairs and Data Flows
MO59
B-1049 Brussels/Belgium
JUST-01-INTERNATIONAL@ec.europa.eu

EFF response to review questionnaire of the EU-US Data Privacy Framework (DPF)

Mr. Bruno Gencarelli,

Thank you for your invitation to provide information and observations on the European Commission's review of the EU-US Data Privacy Framework (DPF). Given the recent developments in US surveillance laws, we focus on these changes and their implications for data privacy, especially concerning non-US persons. This submission does not analyze the DPF itself but highlights critical changes in the US legal framework since July 2023.

Recent changes in US surveillance laws, particularly under the Reforming Intelligence and Securing America Act ("RISAA") and Executive Order 14086 ("EO 14086"), significantly expand the scope of surveillance on non-US persons while failing to address key data privacy concerns. RISAA increases the number of entities that the US government may require to disclose communications pursuant to Section 702 and broaden the purposes for which the US government may collect this data. This risks widespread monitoring, which the lack of effective judicial redress and inadequate oversight mechanisms further exacerbate. EO 14086 regrettably introduces only marginal reforms to US signal intelligence activities, which do not sufficiently protect non-US persons' data privacy rights.

Thank you for considering our comments. Should you have any questions or require further information, please do not hesitate to contact us.

Kind Regards,

Katitza Rodríguez Pereda, Policy Director for Global Privacy
Electronic Frontier Foundation (EFF)

David Greene, Senior Staff Attorney and Civil Liberties Director
Electronic Frontier Foundation (EFF)

Brendan Gilligan, Legal Fellow
Electronic Frontier Foundation (EFF)

**About EFF**
EFF is an international civil society non-governmental organization with over 30,000 members from 88 countries throughout the world. EFF is dedicated to the protection of individuals' privacy, data protection, and free expression in the digital age. EFF engages in strategic litigation and works in a range of global, regional and national policy venues to promote and protect human rights, foster innovation, and empower consumers.

**EFF's History and Expertise Fighting Mass Surveillance in the United States**
EFF has been fighting US mass surveillance programs since 2006, when the program later authorized by Section 702 of the FISA Amendments Act was largely secret and conducted without any public oversight.

EFF filed three lawsuits challenging various aspects of US mass communications surveillance programs. Each of these lawsuits was resolved without any ruling on the merits of the constitutionality of the surveillance programs.

The first, *Hepting v. AT&T*, filed in 2006, challenged the collaboration by AT&T, a major US telecommunications provider, with the US government to copy all internet traffic that flowed through AT&T infrastructure. The case was dismissed as moot after the US Congress granted participating telecoms immunity from liability as part of the FISA Amendments Act of 2008.[1]

The second lawsuit, *Jewel v. National Security Agency*, was filed in 2008 on behalf of the same plaintiffs, all AT&T customers, this time against the US government, claiming violation of both First (freedom of expression) and Fourth (freedom from unreasonable searches and seizures) Amendment rights under the US Constitution, as well as statutory violations.[2] The case was litigated for 14 years with the government consistently contesting the plaintiffs' standing to bring the lawsuit because, it maintained, they could not prove that they had individually been subject to the mass surveillance and also because the courts could not consider or rule on the case without revealing secret national security information, pursuant to a judge-made doctrine known as the "state secrets privilege." Like its predecessor, the case was dismissed, on those grounds, without any consideration of the constitutional questions.

EFF also filed a third case in 2013, *First Unitarian Church of Los Angeles v. NSA*, which challenged a different mass surveillance program, the call detail records collection conducted under the purported authority of section 215 of the USA PATRIOT Act.[3] That lawsuit also asserted claims for violations of First and Fourth Amendment rights with a particular focus on the freedom of association – each of the plaintiffs was an organization with an interest in keeping its membership and other associations private from the government. However, the

[1] *See* EFF, *Hepting v. AT&T*, *available at* https://www.eff.org/cases/hepting.
[2] *See* EFF, *Jewel v. National Security Agency*, *available at* https://www.eff.org/cases/jewel.
[3] *See* EFF, *First Unitarian Church of Los Angeles v. NSA*, *available at* https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa.

constitutional issues presented in that case were never considered by the court either. The case was largely mooted when the US Congress revised the surveillance program in the USA FREEDOM Act of 2014 and then subsequently agreed to destroy most of the records it had collected under the former program. EFF has also consistently advocated for legislative reforms of the statutory authority for these laws and has pursued public records litigation to bring more information to light about them.

**US Courts Do Not Provide An Adequate Forum to Adjudicate Infringements on the Rights of Non-US Persons**

Importantly, each of those cases we brought sought only to vindicate the rights of "US persons" – US citizens, permanent residents, and others physically on US property. Regrettably, under the current prevailing interpretation of the US Constitution, non-US persons do not have Fourth Amendment rights and doubtfully have First Amendment rights.[4] As a result, US courts do not provide an adequate venue for non-US persons to vindicate their rights.

And any concern for the rights of non-US persons is largely absent from the legislative and other public debates around US mass surveillance programs.

**EFF's Global Fight Against Mass Surveillance: Advocating for Minimum Robust Safeguards in the Context of National Security**

People outside the US are mainly concerned, and rightly so, with the scope of surveillance that Section 702 of the Foreign Intelligence Surveillance Act ("Section 702") and Executive Order 12333 ("EO 12333") authorize. As our partners have written, they are concerned about what "the law can be used for, rather than how it can be abused,"[5] though abuses of the law are still relevant. The unrestricted monitoring, collection, storing of personal data, the absence of robust safeguards, including the lack of transparency increases the risk of unchecked surveillance, inadequate judicial redress for affected individuals, and therefore, violations of the right to privacy and data protection.

Globally, EFF has been advocating for minimum robust safeguards, using international human rights law and standards as benchmarks to assess the compliance surveillance laws in the context of national security with human rights principles.[6] Many of such safeguards have been included in the *Schrems I* and *II* decisions, as well as in other EU court rulings on communication surveillance.

EFF has also intervened in the Court of Justice of the European Union (CJEU), the European Court of Human Rights (ECHR), the Inter-American Court of Human Rights to support these

---

[4] *See United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). *See also USAID v. Alliance for Open Society Int'l*, 140 S. Ct. 2082, 2086 (2020) ("it is long settled as a matter of American constitutional law that foreign citizens outside U.S. territory do not possess rights under the U.S. Constitution.").

[5] *Access Now Responds to Privacy Shield Review Questionnaire* (July 5, 2017), *available at* https://www.accessnow.org/wp-content/uploads/2017/07/AN-PSReviewResponse-1.pdf.

[6] *International Principles on the Application of Human Rights to Communications Surveillance* (2014), *available at* https://necessaryandproportionate.org/files/en_principles_2014.pdf.

principles, and before the UN Human Rights Committee. For example, EFF, together with Human Rights Watch, intervened before the UN Human Rights Committee to address significant human rights abuses stemming from the US's expansive electronic surveillance programs. Our supplemental submission underscores the need for the US to acknowledge its extraterritorial obligations to uphold the right to privacy outside their borders under the International Covenant on Civil and Political Rights ("ICCPR").[7]

In the European Union, for instance, EFF, together with Privacy International and Article19, intervened in the case of Pietrzak and others v Poland before the European Court of Human Rights.[8] This case addresses the lack of effective oversight and remedies under Polish law for individuals subjected to secret surveillance by Polish intelligence agencies, since they were under an obligation to provide the subjects of covert surveillance with any information about the data which was gathered about them. On May 28, 2024, the European Court of Human Rights ruled that Poland's secret surveillance regime violated Article 8 of the European Convention on Human Rights, citing several critical shortcomings: the lack of effective oversight by an independent body, the absence of notification to individuals subjected to surveillance, and the broad and indiscriminate retention of communications data without adequate safeguards against abuse. The Court emphasized that the Polish legislation failed to provide necessary protections against excessive and arbitrary interference with the right to private life, highlighting the importance of independent oversight, transparency, and the ability for individuals to seek redress.[9]

And in Latin America, EFF, Article 19, Fundación Karisma, and Privacy International, represented by Berkeley Law's International Human Rights Law Clinic, submitted an amicus brief to the Inter-American Court of Human Rights in the case of Members of José Alvear Restrepo Lawyers' Collective (CAJAR) v. Colombia.[10] The brief demonstrates that Colombia's intelligence law and unlawful communication surveillance practices violate the right to privacy and other human rights under the American Convention on Human Rights. It draws on evidence of targeted and mass surveillance tools employed by the state to emphasize the need for prior judicial authorization, effective independent oversight, and transparency measures. In a landmark ruling, the Inter-American Court concluded that Colombia's intelligence framework must be adjusted to meet Inter-American human rights standards, emphasizing that national

---

[7] *Human Rights Watch and the Electronic Frontier Foundation Supplemental Submission to the Human Rights Committee During its Consideration of the Fourth Periodic Report of the United States* (Feb. 14, 2014), *available at* https://www.hrw.org/news/2014/02/14/human-rights-watch-and-electronic-frontier-foundation-supplemental-submission-human.

[8] Written Submissions of Privacy Int'l, Article 19 and EFF, *Pietrzak v. Poland,* Eur. Ct. H.R. (2020), *available at* https://privacyinternational.org/sites/default/files/2021-08/2020.10.14%20PI%20submission%20Pietrzak%20ao%20ECtHR%20FINAL.pdf.

[9] *Forthcoming public delivery in the case of Pietrzak and Bychawska-Siniarska and Others v. Poland*, European Court of Human Rights (May 21, 2024), *available at* https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-7949776-11079612%22]}.

[10] Brief for Amici Curiae EFF, Article 19, Fundación Karisma, and Privacy International, *CAJAR v. Colombia*, Inter-Am. Ct. H.R. (May 24, 2023), *available at* https://www.eff.org/files/2022/06/03/amicus-brief-ccajar-v.-colombia.pdf.

security cannot justify blanket denial of access to personal information.[11] The court recognized the right to informational self-determination, stating that individuals have the right to access and control their personal data. The ruling set crucial standards for state surveillance practices by intelligence agencies in the region.

In that vein, EFF has been advocating for international human rights law and standards principles. Among others, here are a few key safeguards:[12]

- **Legality**: Any limitation on fundamental rights must be provided for by law, respect the essence of those rights, and meet objectives of general interest or protect the rights and freedoms of others; Surveillance measures must be governed by clear and precise rules, imposing minimum robust safeguards to protect personal data against abuse and unlawful access;
- **Necessity and Proportionality**: Access to personal data by public authorities must be limited to what is strictly necessary and proportionate;
- **Prior Judicial Authorization**: Surveillance measures must be subject to prior judicial authorization. This involves a thorough assessment of the necessity and proportionality of the surveillance, ensuring it is conducted lawfully and only under justified circumstances;
- **Notification:** Individuals subjected to surveillance should be notified as soon as it no longer jeopardizes the purpose of the investigation;.
- **Transparency**: The processes of surveillance and the decisions of oversight bodies must be transparent and subject to public scrutiny. This includes providing notice to individuals who have been subjected to surveillance, enabling them to challenge such actions and seek redress;
- **Oversight**: State surveillance of communications should be subject to independent, effective, and adequately resourced oversight mechanisms that ensure transparency and accountability. Oversight bodies must be independent from the authorities conducting the surveillance, possess appropriate expertise, and be institutionally separated from authorization processes. They should proactively investigate and monitor surveillance activities, require regular reporting from surveillance agencies, and maintain thorough records of surveillance measures. Oversight processes should be transparent, allowing for public scrutiny, and decisions must be subject to appeal or independent review to prevent abuses and ensure compliance with human rights standards.

---

[11] *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" v. Colombia*, Inter-Am. Ct. H.R. (Oct. 18, 2023), *available at* https://www.colectivodeabogados.org/historico-corte-interamericana-encuentra-responsable-internacionalmente-a-colombia-por-violar-el-derecho-a-defender-derechos-humanos/.

[12] *International Principles on the Application of Human Rights to Communications Surveillance* (2014), *available at* https://necessaryandproportionate.org/files/en_principles_2014.pdf. *See also* Privacy International, PI's Guide to International Law and Surveillance (3rd ed. 2021), available at https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf

**Relevant Developments in the US Legal Framework**

**RISAA**

RISAA, which the US Congress passed and President Biden signed into law in April 2024, does nothing to address the deficiencies identified in the *Schrems* cases. Indeed, RISAA not only reauthorizes Section 702, but expands the surveillance the US government is authorized to conduct under Section 702, as well as the larger Foreign Intelligence Surveillance Act ("FISA"): with RISAA, the US is now authorized to target non-US persons' communications in more circumstances than before.

While EFF has concerns about many of RISAA's provisions, there are two that are especially relevant to this commission's request for comment.

The first of these provisions expands Section 702's definition of "electronic communication service provider." Prior to RISAA, Section 702 defined this term to "include essentially anyone who provides a service that facilitates electronic communication of any kind or that otherwise has access to transiting or stored wire or electronic communications or other stored electronic information."[13]

The RISAA provision in question amends the definition of "electronic communication service provider," so that it now also includes "any other service provider who has access to equipment that is being or may be used to transmit or store wire or electronic communications," subject to a handful of specific exceptions.[14] According to the member of Congress who sponsored this amendment, this provision "responds" to a 2023 Foreign Intelligence Surveillance Court of Review, or FISCR, decision, which is not otherwise public.[15] Per reporting from the New York Times, the FISCR decision rejected the US government's argument that a data center qualified as an "electronic communication service provider" under that term's pre-RISAA definition.[16]

But RISAA's new provision goes far beyond data centers and significantly increases the US government's access to non-US persons' communications. This new definition of "electronic

[13] David S. Kris & J. Douglass Wilson, National Security Investigations & Prosecutions § 17.8 (3d Ed. 2019).
[14] 50 U.S.C. § 1881(b)(4).
[15] Rules Committee Hearing H.R. 529, H.R. 7888, H. Res. 1112, H. Res. 1117, 118th Cong. (2:33:53), *available at* https://rules.house.gov/video/rules-committee-hearing-hr-529-hr-7888-h-res-1112-h-res-1117. *See In re* Petition to Set Aside or Modify Directive Issued to [REDACTED], No. FISCR [REDACTED] (FISA Ct. Rev. 2023), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf.
[16] Charlie Savage, *Secret Rift Over Data Center Fueled Push to Expand FISA Surveillance Program*, N.Y. Times (April 17, 2024), https://www.nytimes.com/2024/04/16/us/fisa-surveillance-bill-program.html.

communications service provider" is ill-defined and written so expansively that it potentially reaches any person or company with "access" to "equipment" on which electronic communications travel or are stored, regardless of whether they are a direct provider. This could potentially include landlords, maintenance people, and many others with access to electronic communications. Subject to some restrictions, the US government may compel those entities that qualify as "electronic communication service providers" to produce "foreign intelligence."

The second RISAA provision with which EFF has particular concerns expands the definition of this latter term, "foreign intelligence information." Even before RISAA, "foreign intelligence information" was defined very broadly—for example, "foreign intelligence information" included information regarding a foreign government or territory that "relates to" US national security or foreign affairs (and did not concern a US person).[17] But RISAA added to this broad definition, so that "foreign intelligence" now includes the "international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths," or their precursors.[18]

Throughout the debate over reauthorizing Section 702, EFF advocated against RISAA's expansions and for meaningful reforms. One reform EFF advocated for relevant to this commission's request for comment was a modification of FISA's procedures for handling classified evidence.[19] Reform of these classified evidence procedures—that makes clear that plaintiffs with standing (which is unlikely to include non-US persons) may use FISA's procedures in lawsuits challenging FISA surveillance—is crucial to ensuring US Article III courts may review Section 702's merits.

Unfortunately, RISAA did not reform FISA's procedures for handling classified evidence: US Article III courts remain inhibited from reviewing FISA surveillance in lawsuits challenging it, which undermines the privacy of US and non-US persons alike. As noted above, EFF unsuccessfully advocated in its legal challenges and in amicus curiae briefs in related cases that FISA's classified evidence procedures displaced the state secrets privilege that made many claims against such surveillance nonjusticiable.[20] But US courts have reached contrary results[21] and dismissed these lawsuits.[22]

---

[17] 50 U.S.C. § 1801(e)(2).
[18] 50 U.S.C. § 1801(e)(1)(D).
[19] *See* 50 U.S.C. § 1806(f).
[20] *See generally* Brief for Electronic Frontier Foundation as Amici Curiae Supporting Respondents, Fed. Bureau of Investigation v. Fazaga, 595 U.S. 344 (2022) (No. 20-828), *available at* https://www.eff.org/document/eff-fazaga-scotus-amicus-brief.
[21] *See Fed. Bureau of Investigation v. Fazaga*, 595 U.S. 344 (2022).
[22] *See* Order Requiring Dispositive Motions Briefing, Jewel v. Nat'l Sec. Agency, No. 410, C 08-04373 JSW (N.D. Cal. Aug. 18, 2018) *available at* https://www.eff.org/files/2023/08/29/410_order_requiring_dispositive_motions.pdf; *Jewel v. Nat'l Sec. Agency*, No. C 08-04373 JSW, 2019 WL 11504877 (N.D. Cal. Apr. 25, 2019), *aff'd*, 856 F. App'x 640 (9th Cir. 2021).

**EO 14086 Developments**

EO 14086 is one of many authorities that regulate signals intelligence activities that the executive branch of the US government conducts under its own authority, pursuant to EO 12333. These authorities must be read in concert to understand EO 14086's effects on non-US persons' privacy interests.

Despite EO 14086, the signals intelligence activities the US conducts under EO 12333 do not provide sufficient protections for non-US persons' data and their privacy rights more broadly. At best, EO 14086 imposes marginal reforms on SIGINT activities the US conducts pursuant to EO 12333, which do not substantively improve the protection of non-US persons' data privacy rights.

While EO 14086 requires US signals intelligence collection to advance more precise objectives,[23] the purposes for which the US may collect signals intelligence under EO 14086 remain very broad and allow US intelligence agencies to justify a wide range of activities under the guise of national security. Before President Biden issued EO 14086, intelligence agencies could collect signals intelligence to obtain "foreign intelligence"[24] or "counterintelligence,"[25] support military operations, or protect the safety or enable the recovery of US person captives.[26] EO 14086's legitimate objectives don't prohibit intelligence agencies from collecting signals intelligence to advance any of these preexisting purposes. In fact, some of EO 14086's legitimate objectives may be interpreted as expanding the purposes for which US intelligence agencies can collect signals intelligence. For example, the legitimate objective "ecological change"[27] could be read as broadening the purposes for which US intelligence agencies may collect signals intelligence beyond that which EO 12333's implementing regulations authorize.

The purposes for which EO 14086 prohibits intelligence agencies from collecting signals intelligence only differ in two ways to those that previously existed.[28] First, they assert that US intelligence agencies cannot collect signals intelligence to suppress or restrict "legitimate privacy interests": public US government materials do not define this term, it lacks clarity and precision. Second, EO 14086 prohibits US intelligence agencies from collecting signals intelligence to disadvantage persons based upon their gender identity or to suppress or burden individuals or the press's "free expression of ideas or political opinions."[29]

---

[23] EO 14086, § 2(b)(i), *available at* https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.
[24] DoD Manual 5240.01 ("DOD Manual"), § G.2. (2016), *available at* https://www.eff.org/files/2024/05/28/dod_manual.pdf.
[25] *Id.*
[26] DoD Manual S-5240.01-A ("SIGINT Annex"), § 2.1, *available at* https://www.eff.org/document/sigint-annex. *See also* DOD Manual, § 3.5.f.
[27] EO 14086, § 2(b)(i)((A)(3).
[28] *See* PPD-28 Procedures, § 3, *available at* https://www.eff.org/document/ppd-28-section-4-procedures; SIGINT Annex, § 1.3.e.
[29] EO 14086, § 2(b)(ii).

EO 14086's requirement that the Civil Liberties Protection Officer ("CPLO") "assess" the Director of National Intelligence's priorities also represents a very modest reform that does not safeguard non-US persons' privacy interests.[30] The CPLO only assesses whether the Director's priorities comply with the aforementioned marginal reforms.[31] Further, the CPLO's assessment is non-binding: if the Director of National Intelligence disagrees with the CPLO's assessment, EO 14086 only requires the Director to "include" the CPLO's assessment (and the Director's views) when the Director presents their priorities to the President.[32]

Many of EO 14086's safeguards repackage preexisting regulations which failed to provide sufficient privacy protections. For example, those sections of EO 14086 regulating signals intelligence collection are almost the exact same as those found in the NSA's internal procedures implementing EO 12333.[33]

EO 14086's regulations concerning bulk collection deserve special note[34]: these regulations do not materially differ from those preexisting regulations that provided insufficient protections for non-US persons' privacy. NSA procedures already purported to prioritize targeted over bulk collection.[35] And PPD-28 imposed the same regulations on the purposes for which the US government could conduct bulk collection as EO 14086.[36] Further, EO 14086 authorizes the President to update the purposes for which the US government can conduct bulk collection and even prevent public disclosure of these updated purposes if they deem it would be a risk to US national security.[37]

Also warranting comments are the EO 14086 regulations concerning retention of non-US persons' information ("non-USPI"). While EO 14086 prohibits US intelligence agencies from retaining non-USPI longer than US persons' comparable information,[38] this regulation could be misconstrued without greater context. For example, under EO 12333 US intelligence agencies generally cannot intentionally collect US persons' domestic communications. Further, intelligence agencies are generally prohibited from retaining the domestic communications of US persons in which they have a reasonable expectation of privacy. Non-US persons enjoy neither of these notable protections.

The regulations EO 14086 imposes regarding the retention of non-USPI are also difficult to reconcile with other intelligence agency regulations implementing EO 12333, under which the retention period for non-US persons' communications depends on whether they contain USPI. For example, whereas intelligence agencies may only retain foreign communications to, from, or

[30] *See* EO 14086, § 2(b)(iii).
[31] EO 14086, § 2(b)(iii)(B).
[32] *Id.*
[33] *Compare* EO 14086, § 2(c)(i) *with* SIGINT Annex, § 2.2–2.3.
[34] EO 14086, § 2(c)(ii).
[35] SIGINT Annex, § 2.2.a.(2).
[36] *Compare* EO 14086, § 2(c)(ii)(B) *with* PPD-28 Procedures, § 2.
[37] EO 14086, § 2(c)(ii)(C).
[38] EO 14086, § 2(b)(iii)(A)(2)(a).

about a US person for five years, these agencies "may permanently retain" foreign communications—provided they constitute "foreign intelligence"—when all parties to them are reasonably believed to be non-US persons and from which all USPI has been removed.[39] The retention period for non-USPI cannot be the same as that for USPI when the retention period for foreign communications depends on whether they contain USPI.

It is difficult to assess whether US intelligence agencies' retention of signals intelligence is compatible with the CJEU's standards. The CJEU, particularly in the *Schrems II* decision, emphasized the necessity of clear, precise, and accessible rules to ensure that any interference with fundamental rights be strictly necessary and proportionate.[40] Because EO 14086's regulations are difficult to reconcile with other intelligence agency regulations implementing EO 12333, it is not clear that US intelligence agencies' retention of non-USPI satisfies these standards.

EO 14086 also fails to satisfy the CJEU's oversight and judicial redress requirements.

Starting with oversight, the CJEU has stated that "an independent supervisory authority is an essential component of the protection of individuals with regard to the processing of personal data" and that "this independence is necessary to ensure the effectiveness and reliability of the monitoring of compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data."[41]

Similarly, EO 14086's regime fails to satisfy this standard set forth in the *Tele2 Watson* case, in which the CJEU emphasized that "Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law."[42] The CPLO and DPRC members are not judicial entities but instead are non-independent executive branch officials overseeing executive branch surveillance. EO 14086 thus does not provide non-US persons an independent forum in which they may seek redress, non-US persons lack sufficient judicial redress. As the CJEU emphasized, "According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection."[43]

---

[39] SIGINT Annex, § 4.4.
[40] Case C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020), ¶ 137.
[41] Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (GC Oct. 6, 2015), ¶ 41.
[42] Case C-203/15, Tele2 Sverige AB v. Post- och telestyrelsen, ECLI:EU:C:2016:970 (GC Dec. 21, 2016), ¶ 123.
[43] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559, ¶ 187 (July 16, 2020). *See also* Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen, ECLI:EU:C:2016:970, note 5, ¶ 121..