1 December 2021

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Report on the Remote Audit of Internal Rules Restricting Data Subjects´ Rights under Article 25 of the Regulation (Case 2021-0165)

Executive Summary

Fundamental rights, enshrined in the Charter of Fundamental Rights of the European Union ('Charter'), constitute the core values of the European Union. The **conditions for possible limitations on the exercise of fundamental rights are of utmost importance**, because they determine the extent to which the rights can effectively be enjoyed[1].

Article 52(1) of the Charter states that any limitation on the exercise of the right to personal data protection (Article 8 of the Charter) must be necessary for an objective of general interest or to protect the rights and freedoms of others. In matters relating to the operation of the Union institutions and bodies (`EUIs´), Article 25 of Regulation (EU) 1725/2018 (`Regulation´) states that **Internal Rules may restrict the application of data subjects´ rights**, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard a certain number of legally protected interests.

This remote audit aims at understanding how EUIs[2] have taken into account the **recommendations issued by the EDPS** when drafting their Internal Rules. It further looks into the application of these Internal Rules in practice by examining **actual cases** of EUIs restricting data subjects´ rights[3]. In assessing compliance, the EDPS takes into account in particular the EDPS Guidance on Article 25 of the Regulation of June 2020 ('EDPS Guidance').

The decision to carry out a remote audit on these topics was determined by taking into account the following points:

- The fact that decisions under Article 25 of the Regulation restrict fundamental rights, i.e. represent a **high impact on data subjects**;
- The **high number EUIs concerned**[4] gives a horizontal view on a topic that has proven to be contentious, in particular in complaints relating to access requests under Article 17 of the Regulation.

This general report is published with a view to reporting on the overall results of the audit and providing guidance to all EUIs on best practices identified during the exercise.

- Section 1 of this document gives an overview of instances where EUIs have not adopted or published their Internal Rules yet.
- Section 2 covers guidance issued by the EDPS on Article 25 of the Regulation so far and concludes that this remote audit might contribute to EUIs realising that a (partial) review of their Internal Rules is required, although they followed previously available guidance.
- Section 3 examines the follow-up given by EUIs to recommendations issued by the EDPS in the context of consultations and refers to specificities identified as preliminary findings.
- Section 4 looks at the application of Internal Rules in practice by assessing individual decisions taken to restrict data subject rights (mostly Article 17 of the Regulation). The

[1] *See EDPS Necessity Toolkit and EDPS Proportionality Guidelines.*
[2] *The scope of the audit excludes Executive Agencies.*
[3] *Case 2020-0225 (SG) concerns derogations under Article 25(4) of the Regulation and was dropped from the scope of this audit.*
[4] *Respective EDPS cases had been closed for more than 45 EUIs in March 2021.*

assessment uses criteria contained in a checklist, taking into account pieces of evidence submitted as well as a self-assessment provided.

1. Internal Rules - overview

1.1.1. Background

Pursuant to Article 25 of the Regulation, any restriction has to be either based on a legal act adopted on the basis of the Treaties or, in the absence of such legal basis, in matters relating to the operation of EUIs, on the internal rules ('IR') of the EUIs. This is different from the previous Regulation[5], where restrictions were based on Article 20 directly. The **EUIs should thus ensure that there is a clear legal basis before applying any restriction** and, when this basis is found in IR, they must ensure that they are published in the Official Journal of the European Union.

1.1.2. Findings

When this remote audit was launched on 17 May 2021, **four EUIs had not published any IR**, out of which **three EUIs had not even adopted any IR**.

- "We nevertheless submitted, on 23 March 2021, a draft proposal to your services for opinion... Your services issued their general comments and recommendations on the submitted draft on 20 April 2021... The internal rules are expected to be formally adopted by the Bureau of the (EUI) by the end of 2021."
- "...was approved by the EUI's Administrative Committee at its meeting on 3 May 2021, and will be presented ... for adoption at its meeting on 20 May 2021."
- "The EUI has obtained the EDPS opinion on 12 March 2021 ... and is currently incorporating the EDPS comments ... Once ... consultations are closed, the drafts will be submitted to the Executive Board of the EUI for adoption..."
- "...adopted by the EUI's Management Board on 19 April 2021 ... following its adoption, the Decision is currently being translated into the official languages of the European Union prior to its publication in the Official Journal, which is expected within the coming weeks."

For an overview of the IR in place at all other EUIs, see **Annex 1**.

1.1.3. Recommendations / conclusions

EUIs which have not yet adopted and/or published IR are urged to do so as a matter of urgency, so as to **ensure a clear legal basis before applying any restriction**.

Having such IR in place is not a question of ticking another compliance box, but a pre-condition to legally be in a position to offer e.g. adequate safeguards to whistle-blowers or to protect the rights and freedoms of other data subjects in the context of administrative inquiries if and when required.

---

[5] *On the basis of Article 20 of Regulation (EC) No 45/2001, the EUIs could directly apply a restriction based on that Regulation without the need for internal rules or any other specific legal basis.*

2. Guidance issued by the EDPS

2.1.1. Background

In assessing compliance in the context of this remote audit, the EDPS takes into account in particular the EDPS Guidance on Article 25 of the Regulation ('EDPS Guidance').

2.1.2. Findings

This **EDPS Guidance was issued in June 2020**. The EDPS acknowledges that a number of non-implementation issues identified in the context of this remote audit are linked to the fact that **EUIs, including the EDPS, drafted and adopted their IR before the adoption of the EDPS Guidance**. In doing so, the EDPS understands that they in good faith relied e.g. on earlier EDPS' guidance issued in December 2018, on recommendations made by the EDPS in the context of consultations launched before June 2020 (see section 3 of this Report) or on the wording of the EDPS' own IR adopted in April 2019.

Example: "EUI's Internal rules are built on the model provided in EDPS' Guidance on Article 25 (December 2018) and further amended according to the recommendations of EDPS provided on 20 June 2019. EUI's Internal rules follow the structure as provided in Article 25 of EUDPR and have been published in OJEU on 25 November 2019. EUI's Internal rules are also aligned with the template discussed in the Working Group in coordination with EDPS."

Example: "When (EUI) received the recommendations from EDPS in 2019, we did not believe that we needed to change the wording of the decision. When we consulted EDPS two years ago, the phrasing was accepted by EDPS. We read now that the template from EDPS of 24 June 2020 mention this documentation, however (EUI) was one of the first Agency to adopt its rules on restriction based on the previous template adopted in 2019."

Example: "Most of the internal rules in question were adopted at the time or immediately after Regulation (EU) 2018/1725 started applying in December 2018. Therefore, they were amongst the first internal rules adopted by the EUIs under Article 25 of Regulation (EU) 2018/1725. When those internal rules were drafted and introduced into adoption procedure, there was very little practical experience with the implementation of Article 25 in the EUIs. Furthermore, the EDPS Guidance on Article 25 of Regulation (EU) 2018/1725 (released on 20 December 2018) has not yet been available."

Example: "I would like to note that Art. 4(d) of the (EUI) internal rules is exact the same wording of the corresponding Articles of the EDPS internal rules on restrictions of data subjects rights published on the OJ."

Example: "We also noted at that time that the EDPS Decision also used a similar approach in the final article, without a specific reference in the recitals."

2.1.3. Recommendations / conclusions

Recommendation 7 of the EDPS Guidance reads "Review your internal rules periodically and when necessary". This remote audit might thus also contribute to EUIs realising that **a (partial) review of their IR is required**, although they did their best to follow previously available guidance.

Example: "From a practical perspective, as these rules have never been used so far, and given the procedural aspects involved in a review (EUI's top management approval, translation in all EU languages and publication), EUI has not considered this update as a priority for now, and rather had contemplated a review in a couple of years pending the effective use of these restrictions which may then lead to the identification of further necessary adjustments to the rules. However, should this update be seen as a priority by the EDPS, EUI stands ready to make the necessary (limited) amendment shortly.

All preliminary findings were shared with the respective EUIs with a view to allowing them to confirm the findings as well as to explain and complete any evidence collected, where required. Following this consultation on the preliminary findings of this remote audit for each EUI, four EUIs have already **undertaken commitments to amend their IR accordingly** to ensure full compliance.

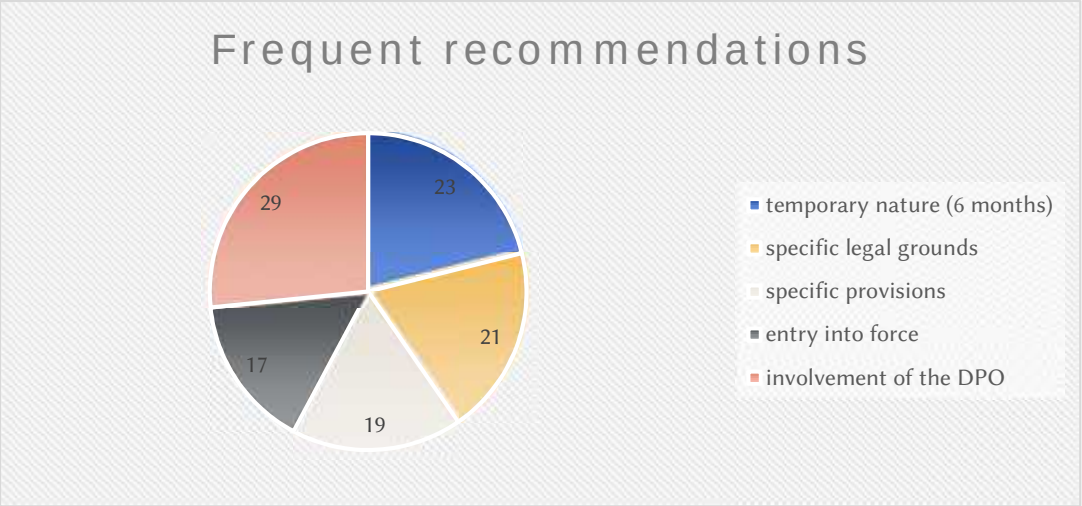
Where the audit reveals that the implementation of the IR of a particular EUI is not in conformity with Article 25 of the Regulation, a separate case will be opened to follow-up. This general report is published in order to report on the overall results of the audit and provide guidance to all EUIs on best practices identified during the exercise.

3. Follow-up given to EDPS recommendations

Protection of personal data is a fundamental right, which contains 'rights within the right' such as the right of information, access, rectification, portability, right to erasure etc. These rights should be strictly respected. However, according to EU secondary legislation they could be restricted in exceptional circumstances and with the safeguards laid down in the Regulation. EUIs should adopt such restrictions only where strictly necessary and always based on a legal act or, in the absence of such a legal act, on **IR adopted by the highest level of management and published in the Official Journal of the European Union**.

Restrictions carried out on the basis of IR are only possible in matters relating to the operation of EUIs. Each restriction should be linked to the applicable legal grounds for restricting an individual's (data subject) rights as provided for in Article 25(1) of the Regulation. **Consulting the EDPS when drawing up IR is required**[6]. Since the entry into force of the Regulation in December 2018, **the EDPS has been consulted by over 50 EUIs**.

This remote audit aims at understanding how EUIs have taken into account the recommendations issued by the EDPS when drafting their Internal Rules[7]. The EDPS responded to each consultation separately by issuing a decision vis-à-vis the EUI concerned. Some recommendations were specific to the particular EUI or to the wording or structure of the draft IR submitted, others applied more generally to several EUI draft IR.



From these general recommendations, **the most frequently issued recommendation relates to the involvement of the DPO** (29 cases). It is closely followed by the temporary nature of restrictions and a six month review cycle (23 cases) and recommendations to specify which of the grounds provided for in Article 25(1) of the Regulation the EUI wants to rely on and/or, in doing so, to refer only to the grounds from the exhaustive list set out therein (21 cases). Runners up are

[6] *Article 41(2) of the Regulation: "The Union institutions and bodies shall consult the European Data Protection Supervisor when drawing up the internal rules referred to in Article 25."*
[7] *The scope of this audit excludes Executive Agencies.*

recommendations on creating specific provisions under Article 25(2) (19 cases) and recommendations on the entry into force of the IR (17 cases)[8].

[8] *Other general recommendations are on data breaches (12 cases), data portability (8 cases), the format and publication of the data protection notice (8 cases) and medical content (6 cases).*

3.1. Involvement of the DPO

3.1.1. Background

In 29 consultation cases, the EDPS recommended the documented involvement of the DPO in all stages of the procedure.

> *Example: "The EDPS welcomes the fact that, according to recital X and Article Y, the Data Protection Officer (DPO) will be informed about applied restrictions. Under these provisions, the DPO will be informed 'at the moment of deferral and during the revisions' (Recital X) or 'whenever the controller restricts the application of data subjects' rights, or extends the restriction' (Article Y). The EDPS recommends adding the active documented involvement of the DPO throughout the entire procedure into the text."*

This recommendation is actually two-pronged:

1. The DPO needs to be involved in all stages of the procedure, **not just once the decision to restrict has already been taken** or applied vis-à-vis the data subject;
2. This DPO involvement needs to be **documented** throughout the procedure.

Under Article 44 of the **Regulation**, EUIs "shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data". It is difficult to conceive situations which by their nature "relate" more to the protection of personal data than the restriction of data subject rights: The conditions for possible limitations on the exercise of fundamental rights are of utmost importance, because they determine the extent to which the rights can effectively be enjoyed[9].

It is consequently not surprising that the **EDPS Guidance** highlights the importance of involving the DPO throughout the procedure, starting with the design of the procedure, determining the possible application and the required safeguards in individual cases as well as review activities:

- §46 of the EDPS Guidance states that "As a matter of good practice, the DPO should be involved in the drafting of the internal rules, the 'proportionality and necessity test assessment note' and in the subsequent reviews."
- Furthermore, recital 22 of the template IR contained in the EDPS Guidance reads: "To guarantee utmost protection of the rights and freedoms of data subjects and in accordance with Article 44(1) of the Regulation, the DPO should be consulted in due time of any restrictions that may be applied and verify their compliance with this Decision."
- Also, §26 of the EDPS Guidance aims at involving the DPO in assessing the necessity and proportionality of each restrictive decision by stipulating "...the DPO should always be informed and, if possible, involved in the assessment."

Regarding the **timing of the DPO's involvement**, Article 5 of the template IR entitled "Involvement of the Data Protection Officer" contained in the EDPS Guidance is not particularly explicit on involving the DPO ***before*** **the controller actually takes the decision** to restrict data subject rights in a particular case. However, Recommendation R6 of the EDPS Guidance clearly states the following: "Consult the DPO *before* and during the restriction" (emphasis added) and,

---

[9] *See EDPS Necessity Toolkit and EDPS Proportionality Guidelines.*

in a footnote, further explains that "The controller should involve the DPO throughout the procedure and document this consultation".

Article 5(3) of the template IR states that "The [EUI] shall **document the involvement of the DPO** in the application of restrictions, including what information is shared with him or her."

3.1.2. Findings

A total of 14 EUIs had not included a requirement to involve the DPO throughout the procedure in the text of their IR. Most of these included a reference to ***informing*** **the DPO, but only after a decision to restrict data subjects' rights has been taken**.

> *Example: "The obligation to consult the DPO also flows directly from article 44(1) of Regulation 2018/1725 according to which the institution shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The decision on internal dispositions concerning the DPO clarifies in its article 5(2) that the DPO has access to all data processed and that the controller has the obligation to assist the DPO in the performance of his duties. The decision on internal rules concerning restrictions, furthermore, makes sure that the DPO is involved through the ad hoc register of all restrictions to the rights of data subjects. These different articles read together assure that the DPO is informed, has access to the relevant data when needed and has the possibility to verify the proper application of a restriction."*
>
> *Example: "Our understanding was that this recommendation focused on the documentation of the DPO's involvement rather than on the exact timing of his involvement, and did not specify as above that the DPO must be informed "already before deciding on a restriction". The Regulation 2018/1725 does not provide for such specific obligation either to involve the DPO before deciding on all restrictions. ...As regards restrictions in a specific case, decision to restrict is entirely left to the case handler who is acting on behalf of the (EUI), as restrictions in this context are done on case specific grounds. The DPO shall be regularly informed of the restrictions..."*

Two EUIs had included the above requirement in the text of their IR, but had failed to include a requirement to *document* such involvement.

> *Example: "...does not provide for (our) DPO to be consulted prior to the application of a restriction. ... Once a restriction is applied, (our) DPO is automatically informed thereof in (our) case management system...".*
>
> *Example: "When we consulted EDPS two years ago, the phrasing was accepted by EDPS. We read now that the template from EDPS of 24 June 2020 mention this documentation, however (we were) one of the first ... to adopt its rules on restriction based on the previous template adopted in 2019."*

Six EUIs claimed that, whilst their IR contained no explicit rule on this, the **DPO was de facto involved**.

> *Example: "... the recommendation to "document the involvement of the DPO" was in the same vein understood as an element, possibly better placed outside the rules and as such not necessarily to be integrated in writing in the text of the rules, but fulfilled by documenting the involvement and discussions or advise of the DPO in the respective files of the business area*

(internal controller) once conducting the proportionality test before applying a restriction (e.g. the Internal Note for the necessity and proportionality test will document the consultation of the DPO)...".

Four EUIs were able to provide evidence that this was indeed the case through demonstrating their DPO´s involvement in an actual decision by providing **template documents clearly referring to the requirement to involve the DPO** before a decision is taken (see **Annex 3** for inspiration).

Example in which a routing slip documented the DPO´s involvement: "...in our practice, the DPO is involved during the whole procedure... The DPO was involved in all steps, including information of the data subject about the lifting of the restrictions. Advise of the DPO was always sought before each step of the process and no decision has been taken without the approval of DPO and data controller."

Example: "The DPO is indeed involved throughout the procedure ...From a practical point of view, (EUI) has already in place instructions for the DP coordinators in case that a restriction applies. This has been integrated in one of the Internal (EUI) documents and in Necessity and Proportionality Test Template (see attachments)..."

Two EUIs argued that the involvement of the DPO would be **covered by their Implementing Rules**, which would further outline the role of their DPO.

Example: "...according to the Data Protection Annual Work Programme, prepared by the DPO in collaboration with (EUI) controllers, Implementing Rules pursuant to Article 45.3 of Regulation (EU) 2018/1725 are planned for this year 2021, which will reflect all considerations on the involvement of the DPO in more detail."

Example: "...the (EUI) guidelines on data protection (currently under revision) would complement the provision of the (EUI) decision on this point, clarifying that the DPO is informed of data subject requests and consulted, where necessary."

Another EUI relied on **oral, i.e. undocumented consultation** of the DPO.

Example: "The recommendation of the EDPS with regard to the involvement of the DPO has been taken into account in the sense that the requirement to involve the DPO is an internal practice that certainly has been followed in the few cases we had so far. A consultation of the DPO can, however, also take place orally."

In the context of this remote audit, the EDPS relied on such documentation to audit the implementation of EDPS recommendations in practice (see **Annex 2** for the kind of evidence requested). In the example above, given the oral nature of DPO consultations and the absence of e.g. an internal note to the file documenting the respective advice given, the implementation of certain EDPS recommendations cannot be verified in the context of the remote audit.

3.1.3. Recommendations / conclusions

To ensure proper involvement of the DPO in the sense of Article 44 of the Regulation, Recommendation R6 of the EDPS Guidance establishes the need to "Consult the DPO *before* and during the restriction" (emphasis added) and states that "The controller should involve the DPO throughout the procedure and document this consultation".

Timing: This recommendation aims at making sure that the controller benefits from the DPO´s input **before any decision to restrict data subjects' rights is taken**, e.g. when assessing the necessity and proportionality of the measure or to ensure consistency with precedents. For most cases, an independent, ex post factum *review* of the application of restrictions by the DPO will not be able to ensure compliance in the same way.

- One way to ensure de facto involvement of the DPO is to use **templates** containing the requirement to involve the DPO. However, the use of these templates should be based on a provision in the IR, as practices might change and not everybody implementing the IR may necessarily be aware of the existence of templates.

- Similar reasoning applies to regulating the involvement of the DPO only in the **Implementing Rules**, without an explicit reference in the IR to the requirement to involve the DPO and document this involvement. Furthermore, it is important, from the perspective of data subjects reading the IR, to have a complete overview also of the procedural elements of a possible restriction, such as the involvement of the DPO, without having to search through other rules laid down by the EUI – even more so because those rules might not be published in the Official Journal of the European Union and therefore possibly not as easily accessible to data subjects.

However, in very particular situations (e.g. decisions on indirect access by the medical service which are determined by the medical condition of the requestor), the DPO might not be able to provide relevant input. Also, in big EUIs, there might be a need to delegate this to data protection coordinators (DPCs). **These exceptions should be made explicit in the IR**.

Documentation: For accountability purposes, to facilitate dealing with precedents and to ensure a smooth transition in case a new DPO is designated, the involvement of the DPO should be documented **in writing**.

The EDPS relied on such documentation to audit the implementation of EDPS recommendations in practice (see Annex 2 for the kind of evidence requested). Where DPO consultations are merely done orally and are not documented, **e.g. in an internal note to the file** documenting the respective advice given, the implementation of certain EDPS recommendations cannot be verified in the context of this remote audit.

3.2. Temporary nature of restrictions: Six months review cycle

3.2.1. Background

In 23 cases, following consultation by the EUI concerned, the EDPS issued recommendations that data subjects' rights be restricted only temporarily and that such decision be reviewed every six months.

> *Example regarding a template submitted by several Agencies: "In relation to the necessity principle, the EDPS underlines that restrictions should be temporary and be lifted when their causes no longer apply. ... in some situations, the EUIs adhering to this template will only asses the need to maintain the restriction on an annual basis, which appears to be too long. The EUIs adhering to this template should apply the six months review cycle in all situations."*

§18 of the EDPS Guidance notes that "To be lawful, any limitation on the exercise of the fundamental rights protected by the Charter must comply with the following criteria, laid down in Article 52(1) of the Charter: ... it must be **necessary**...".

Recommendation R5 of the EDPS Guidance states that "Restrictions should be **temporary and be lifted when their causes no longer apply**".

- Article 4(2) of the template IR contained in EDPS Guidance entitled "Safeguards and storage periods" states consequently that "Restrictions shall be lifted as soon as the circumstances that justify them no longer apply."
- Referring to the necessity and proportionality note, §26 of the EDPS Guidance stipulates that "The controller should revise said note when necessary (Annex III); the DPO should always be informed and, if possible, involved in the assessment".
- According to recital 21 of the template IR: "The [EUI] should lift the restriction as soon as the conditions that justify the restriction no longer apply, and assess those conditions on a regular basis."

Article 4(1) of the template IR entitled "Safeguards and storage periods" states that "The safeguards shall include: ... (d) due monitoring of restrictions and a periodic review of their application. The reviews referred to in point (d) shall be conducted at least **every six months**."

3.2.2. Findings

Seven EUIs had not implemented the recommendation, as their IR had not provided for the requirement to restrict data subject rights only temporarily and/or to review such a decision every six months.

> *Example: "As regards Art.4(d) of (our) internal rules, EDPS commended "The EDPS recommends adjusting this review period to every six months, and reminds that in such cases a necessity/proportionality assessment should be conducted". I have interpreted this sentence in the sense that EDPS recommended ... to modify the review period and reminded the Controller to conduct a necessity/proportionality test in such cases. I did not intend this part of the recommendation as text to be inserted in the rules."*

One EUI argued that the period of six months was impractical and not flexible enough.

> *Example: "...explicitly setting out a review 'every 6 months' is very strict in terms of timing and we considered that it could not provide enough flexibility for us. We thus opted for a period that would oblige (us) to review restrictions on a relatively short term while at the same time without risking any infringements. Indeed, the choice of the words "at least" does not prescribe that the review of the restriction must necessarily be done in a one-year period, as it does not exclude a review every six months (or even every three months) as proposed. Where necessary, as based on the relevant circumstances of the case at hand, the review should be done in a shorter period. This stands in harmony with recital 11 of the Preamble to the Internal Rules, according to which "(We) should periodically monitor that the conditions that justify the restriction apply and lift the restriction as far as they no longer apply". Through the prism of a systemic/contextual interpretation of all relevant legal provisions, the cited caveat "as far as they [the conditions] no longer apply" must then be seen as the overarching obligation, where the "once a year" period must be regarded as a more concrete assurance to this ultimate purpose of ensuring that restrictions are lifted as soon as they stop applying. ...*
>
> *Furthermore, we here recall that (we are) ... of a relatively small size, and the number of potential restriction of data subject rights would be expected to be very limited, what implies in practical terms that, should a case arise, special utmost attention would be devoted to such."*

One EUI saw **no need for a regular review at all**:

> *"As regards the restrictions of those rights, there are sufficient safeguards in place so that such a review does not appear necessary. Indeed, once the (EUI) notifies to a data subject the decision not to grant his/her right to access/erasure/restriction of processing, the data subject can exercise his/her right to lodge a complaint with the European Data Protection Supervisor, and the right to an effective judicial remedy before the Court of Justice. In addition, the data subject also has the possibility to exercise his/her rights (that have in the past not been granted by the (EUI)) anew at a later stage if/when he/she wishes to do so. Consequently, it appears that the data subject would have sufficient legal means at his/her disposal that would safeguard his/her rights under Regulation 2018/1725."*

Another EUI did not see such a need where access to the personal data was refused on the basis of **Article 17(4) of the Regulation**:

> *"...en l'espèce, la demande d'accès a été rejetée, non seulement en application d'une limitation au sens de l'article 25 du règlement 2018/1725, mais également, et même en premier lieu, sur le fondement de **l'article 17, paragraphe 4**, de ce règlement. Ce dernier article prévoit, non pas une limitation au sens dudit article 25, mais une base juridique autonome permettant que l'accès à des données à caractère personnel soit refusé. ...l'**obligation de révision périodique** ... **ne s'y applique pas**. Il s'ensuit que, en l'espèce, une révision périodique de la limitation appliquée ne s'impose pas pour continuer à justifier le rejet de la demande d'accès, dès lors que ce rejet trouve, en tout état de cause, son fondement juridique dans l'article 17, paragraphe 4, du règlement 2018/1725.*

Two EUIs argued that it was **impossible to revise** the relevant decisions every six months, due to the nature of the processing operation concerned:

Example: "...in case of medical files a restriction can be lifted only in cases of new request of access, as Medical Service has no means to regularly evaluate the state of health of the data subject concerned to be able to assess that restriction is no longer applicable."

Example: "Due to the nature of the restriction, that in the case concerned only refers to the name of other persons, under no circumstances the reasoning for its existence would cease to apply. Therefore, (EUI) does not conduct a regular monitoring of these cases."

3.2.3. Recommendations / conclusions

The EDPS acknowledges that reviewing a decision every 6 months is "very strict in terms of timing" – however, the motivation behind this is to ensure that restrictions to data subject rights are lifted as soon as possible, once they are no longer needed. Where such a restriction is no longer necessary, the controller is obliged to lift it. It cannot be left to the data subject to ensure lawfulness by complaining to the EDPS or seeking some form of legal remedy.

Suffice it to note that Article 52(1) of the Charter states that any limitation on the exercise of the right to personal data protection (Article 8 of the Charter) must be *necessary* for an objective of general interest or to protect the rights and freedoms of others. In fixing a longer revision period, EUIs might not be able to ensure this in every case.

For transparency reasons, where the nature of a particular processing operation exceptionally makes a regular review impossible or pointless, this should be clarified in the text of the IR. This is particularly true where a review is conditional on a new request for access to be launched by the data subject concerned.

3.3. Specifying the grounds in Article 25(1) of the Regulation

3.3.1. Background

In 21 cases, the EDPS issued recommendations:

- to specify which of the grounds provided for in Article 25(1) of the Regulation[10] the EUI wants to rely on and/or
- in doing so, to refer only to the grounds from the exhaustive list set out therein.

> *Example: "The EDPS underlines that the grounds for restriction listed in Article 3 of the draft internal rules should only reflect the specific processing operations where the restrictions may take place. As an example, restrictions of data subject rights when conducting administrative inquiries and disciplinary proceedings under Article 86 of the Staff Regulations may be grounded on Article 25(1)(b) and (h) of the Regulation..."*

§50 of the EDPS Guidance states that "The scope of the restrictions should also be specified, i.e. which rights are concerned and how far they are going to be limited, for instance, the restriction will only concern access rights, or alternatively that it may concern access, rectification and confidentiality of communication."

> *Example regarding a template submitted by several Agencies: "... restrictions to the right of access regarding selection procedures and staff evaluation (Article 1(2) of the draft internal rules) do not seem necessary. The EUIs adhering to this template can ensure the 'secrecy of the jury' in recruitment procedures by referring to the jury in an aggregated manner when evaluating candidates, instead of having separate assessments per juror. There seems to be no obvious use case for restricting the right of access in staff evaluation procedures either. The 360° evaluation procedures should be implemented in such a way that no personal data from the data subjects giving anonymous feedback is collected. The EDPS, therefore, recommends that the EUIs adhering to this template remove the possibility to restrict this right in the abovementioned situations. ...*
> *The same remarks seem applicable to the restrictions to the right of access regarding public procurement procedures. In this field, the EDPS has only accepted restrictions to the right to rectification of personal data after the closing date for submissions. ..."*

3.3.2. Findings

In eight cases, EUIs had not followed up on this recommendation and their IR had not listed the specific processing operations they perform or expect to perform in the light of the grounds for restrictions. Most non-compliant EUIs had used blanket references to Article 25 of the Regulation, thus not linking each specific processing purpose with the applicable ground for restriction of data subjects' rights.

> *Example: "Article 25(1) EUDPR lists several grounds for restrictions but does not require to determine ex ante which ground to use. As is intended by Art. 25, (EUI) intends to rely on one or the other grounds depending on the facts of the case at hand. (EUI) is not sure about the*

[10] *See Section 4.3 of the EDPS Guidance for details on individual grounds listed in Article 25(1) of the Regulation.*

reason and added value of narrowing down the options offered by the law. What if the need arises to rely on a ground which we did not pre-select but which is foreseen by the law? Would we not be allowed to rely on it in such circumstances? Moreover, if (EUI) were required to amend the Internal Rules, translation into all official languages would be required which, especially against the arguments outlined above, we would not consider proportionate. Perhaps there is an element we are missing, in which case we would be grateful if you could let us know.

In other cases, EUIs defended their choice to keep certain grounds from Article 25(1) of the Regulation in the text of their IR in the light of the specific processing operations they perform or expect to perform.

Example: "The (EUI) considers appropriate to keep ...the reference to Article 25(1)(e) of Regulation (EU) 2018/1725 (EUDPR) ("the protection of judicial independence and judicial proceedings") as a possible ground for restriction because the (EUI) may be requested by the CJEU or national courts to restrict data subject rights in the context of judicial proceedings. ... a scenario is envisaged where the subject of disciplinary proceedings is at the same time subject of criminal prosecution in a given Member State relating to the same facts that have given rise to disciplinary proceedings. ... Considering that judicial proceedings are confidential ...and with a view to preserve judicial independence and the well-functioning of judicial proceedings, the (EUI) could in such cases be obliged to (temporarily) restrict information to the data subjects involved in the administrative inquiries/disciplinary proceedings."

Example: "...the authors followed the input given by the service where the operational side deemed necessary and proportionate to lay down the internal rules allowing the applicability of the restrictions for the purpose of conducting selection procedures. Ultimately, the necessity to regulate it in the proposed format was confirmed by the decision of the ..., a supreme authority of the (EUI)'s administration."

Example regarding a recommendation to remove the possibility to restrict the communication of personal data breaches to the data subject in the framework of anti-harassment procedures: "...depending on the data subject concerned and its position in the procedure, disclosure of a data breach in the context of anti-harassment procedures may also jeopardise the results of the process. Foreseeing a plain and undistinguished exclusion could lead to overlooking the risks to the rights and freedoms of natural persons often involved in these proceedings, at least for some. The documented justification, supported by appropriate assessment of necessity and proportionality as defined in Article 7(1) would secure in our view the soundness of the judgement over the particular case."

3.3.3. Recommendations / conclusions

Under Article 25(5) of the Regulation, "Internal rules referred to in paragraphs 1, 3 and 4 shall be **clear and precise acts of general application**, intended to produce legal effects vis-à-vis data subjects...".

The grounds for restrictions listed by EUIs should therefore be framed in the light of the specific processing operations they perform or reasonably expect to perform and each specific processing purpose should be linked with the applicable ground for restriction of data subjects' rights. Article 2(1) of the template IR contained in the EDPS Guidance contains an indicate overview of how this can be achieved.

3.4. Specific provisions under Article 25(2) of the Regulation

3.4.1. Background

In 19 cases, the EDPS recommended that the IR contain specific provisions as to the scope of the restrictions introduced and invited EUIs to thus specify which rights were concerned and to what extent they were going to be restricted[11].

> *Example: "...the EDPS recommends that the risks to the rights and freedoms of data subjects (stated in Article 25(2)(g) of the Regulation) be clearly included in the draft internal rules, alongside the assessment of the necessity and proportionality of the restriction (including the obligation for documentation). The EDPS also highlights that one of the novelties of the Regulation is the assessment performed by the controller not only regarding the risks posed to the controller itself, but also the risks to the rights and freedoms of the persons affected. These are related, but not necessarily identical. Therefore and as mentioned above, the internal rules should mention the risks to the rights and freedoms of data subjects whose rights may be restricted."*

§51 EDPS Guidance notes that "As far as possible, the internal rules should link the processing operation, the categories of personal data concerned, the scope of the restrictions and the rights that will be restricted. For example, possible restrictions of the right of access to data for alleged harassers in anti-harassment procedures, where this is necessary to protect other persons."

3.4.2. Findings

In 11 instances, IR had not contained provisions specifying which rights were concerned and to what extent they were going to be restricted. Some non-compliant EUIs had used blanket references to Article 25 of the Regulation (see also above, section 1.3.2.).

In some instances, specifications are included in the **recitals of the IR** rather than in the normative part of the IR.

> *Example: "In addition, as regard the storage period... was in the process of being revised at the time of adoption of the Decision and a very precise reference to the storage period would have required to review the Decision 6 months after its adoption, while including items listed in Article 25(2) in recitals rather than in the enacting terms of the Decision is also in line with Article 25(2)."*
>
> *Example: "On Article 25(2) of Regulation (EU) 2018/1725: That provision requires a legal act or internal rule to contain 'specific provisions' with regard to certain areas, thereafter listed, 'where relevant'. The (EUI) mentioned some of these areas in the recitals, some in the enacting terms of the various internal rules.* Recommendations / conclusions

In other instances, **specification was left to the individual restrictive decision**:

[11] *See also Checklist "Specific provisions to be included in internal rules governing restrictions of data subject rights" on p. 3 of the EDPS Guidance.*

Example: "It was deemed to be appropriate (as allowed by the drafting itself of Article 25(2) of Regulation (EU) 2018/1725) to leave the specifications of certain areas to the actual (individual) restriction decisions. In those individual decisions, adopted on the basis of the internal rules, the relevance of each specific relevant area can be better assessed (on a case-by-case basis and following a necessity and proportionality assessment)."

3.4.3. Recommendations / conclusions

Article 25(2) of the Regulation stipulates that "In particular, any legal act or internal rule referred to in paragraph 1 shall contain specific provisions, where relevant, as to..." a number of elements.

It is true that such specifications "shall be contained *where relevant*". However, where they are relevant, they shall be contained in "any legal act or internal rule referred to in paragraph 1", i.e. in the IR themselves, not in the individual decision.

Article 2(1) of the template IR contained in the EDPS Guidance contains an indicate overview of how this can be achieved.

3.5. Entry into force of the internal rules

3.5.1. Background

Article 25(5) of the Regulation stipulates that "Internal rules referred to in paragraphs 1, 3 and 4 shall be … subject to **publication in the Official Journal of the European Union**." (emphasis added).

Article 9 entitled "Entry into force" of the template IR contained in the EDPS Guidance suggests the following wording: "This Decision shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union."

In 17 cases[12], the EDPS recommended revising the initially foreseen date of entry into force of the IR or inserting an explanatory recital, where urgency would require a deviation from the **standard practice** for legal acts, which is entry into force on the **twentieth day after publication** in the Official Journal.

> *Example EASA: "Article X provides for entry into force of the decision on the day following its publication in the Official Journal. We note that this represents a departure from standard practice that is justified only in exceptional cases of urgency. The reasons justifying it are also usually documented in a recital. We recommend checking whether urgent entry into force is necessary. If it is, we recommend inserting an explanatory recital."*
>
> *Example EEA: "Article 9 provides that the decision enters into force on the day following its publication in the Official Journal. The EDPS emphasises that these internal rules would allow for the restriction of fundamental aspects of the right to data protection. Therefore, it should be considered if it would not be appropriate for the decision to enter into force on the twentieth day after publication into the Official Journal, as is standard practice for legislative texts. If urgent entry into force is necessary, we recommend inserting an explanatory recital."*

3.5.2. Findings

Five EUIs had not implemented the recommendation and their IR had continued to provide for entry into force of the decision **on the day or the day following its publication** in the Official Journal.

> *Example: "…the Decision on Article 25 Rules was needed in order to ensure that data subjects' rights would be adequately safeguarded in the event of any potential request within the context of ongoing disciplinary proceedings. We didn't want to include a new recital in order not to diverge too much from the text of the template as agreed in the DPO network, as well as from the text of similar rules adopted by other EUIs."*

Out of those five EUIs, two EUIs had inserted a justification for early entry into force of their IR (on the day following that of its publication in the Official Journal) in an explanatory recital.

---

[12] *EDPS replies to a number of consultations launched before entry into force of Regulation 2018/1725 (e.g. EC IAS) did not include such recommendation.*

Example: "Following, in particular the recommendation concerning Article 9 we have inserted explanatory Recital 17 to the Rules, which explains the need of urgency, and reads as follows: "Regulation (EU) 2018/1725 replaces Regulation (EC) No 45/2001 of the European Parliament and of the Council, without any transitional period, from the date on which it enters into force. The possibility to apply restrictions to certain rights of data subjects was provided for in Regulation (EC) No 45/2001. In order to avoid jeopardising Agency's tasks and activities, this Decision should enter into force on the day following that of its publication in the Official Journal of the European Union."

Example: "...we kept the entry into force as such and introduced, as recommended by the EDPS, a relevant recital in the final text of the IR (recital (15): "Due to the importance of the internal rules for the protection of data subject's rights, the Decision should enter into force as soon as possible after its publication in the Official Journal of the European Union").

One EUI correctly noted that Article 10 of the EDPS' IR of April 2019 states: "This Decision shall enter into force on the day of its publication in the Official Journal of the European Union", without any explanatory recital justifying this.

"We also noted at that time that the EDPS Decision also used a similar approach in the final article, without a specific reference in the recitals."

3.5.3. Recommendations / conclusions

Regarding IR that came into force in the meantime, there is no use crying over spilled milk.

Recommendation R7 of the EDPS Guidance reads: "Review your internal rules periodically and when necessary". This remote audit might thus also contribute to some EUIs realising that a (partial) review of their IR is required.

When EUIs review their IR, they should be aware (even if they have not received a respective recommendation) of the standard practice for legal acts (entry into force on the **twentieth day after publication** in the Official Journal) and the need to insert an explanatory recital, where urgency would require a deviation from this standard practice.

3.6. Data breaches

3.6.1. Background

In 12 cases, the EDPS issued recommendations related to the communication of personal data breaches to the data subject[13].

> *Example: "Article X of the draft internal rules allows the (EUI) to restrict the communication of personal data breaches to the data subject in the framework of its anti-harassment procedures. However, in this context it is unclear which of the grounds of Article 25(1) of the Regulation would require restricting communication of personal data breaches. Therefore, the EDPS recommends adapting Article 8 to remove the possibility to restrict the communication of personal data breaches to the data subject in the framework of anti-harassment procedures."*

According to §16 of the EDPS Guidance, "Articles 35 and 36 of the Regulation can also be restricted: these provisions concern the communication of a data breach to the data subject and the confidentiality of electronic communications. Given that a restriction to the confidentiality of electronic communications may interfere with the essence of the right to privacy, it is only in extraordinary circumstances that this right can be restricted."

Article 7 of the template IR contained in the EDPS Guidance is entitled "Communication of a personal data breach to the data subject" and reads as follows:

> 1. Where the [EUI] is under an obligation to communicate a data breach under Article 35(1) of the Regulation, it may, in exceptional circumstances, restrict such communication wholly or partly. It shall document in a note the reasons for the restriction, the legal ground for it under Article 2 and an assessment of its necessity and proportionality. The note shall be communicated to the EDPS at the time of the notification of the personal data breach.
>
> 2. Where the reasons for the restriction no longer apply, the [EUI] shall communicate the personal data breach to the data subject concerned and inform him or her of the principal reasons for the restriction and of his or her right to lodge a complaint with the EDPS.

3.6.2. Findings

All but one EUIs had implemented the respective recommendations or had adapted the wording of their IR to the wording suggested in Article 7 of the template IR contained in the EDPS Guidance quoted above.

> *"Regarding recommendation to remove the possibility to restrict the communication of data breaches in the context of anti-harassment procedures: ... it was adapted adding some words: formal and informal procedures for dealing with harassment. Restrictions may be based on Article 25(1)(b), (d), (f) and (h) of Regulation (EU) 2018/1725. We kept this specificity only for the four cases where the communication could interfere with the harassment cases and possibly*

[13] *See the EDPS Guidelines of February 2020 on personal data and electronic communications in the EU institutions (eCommunications guidelines).*

invalidate the completion of the investigations, revealing details that would jeopardize the whole process and put on risk the identity of the data subjects: …".

3.6.3. Recommendations / conclusions

None.

3.7. Data portability

3.7.1. Background

In eight cases, the EDPS recommended omitting the reference to the restriction of the right to portability (Article 22 of the Regulation).

> *Example: "Article 1(1) of the draft internal rules mentions restrictions to data subjects' rights pursuant to Articles 4, 14 to 22, 35 and 36 of the Regulation 2018/1725. Despite being referred in Article 1(1) of the draft internal rules, the restriction of the right to portability (Article 22 of the Regulation) does not seem necessary in the context of the EUIs adhering to this template' activities.*

As outlined in §14 of the EDPS Guidance, "While the Regulation provides for the possibility to restrict the right to data portability, EUIs should keep in mind that its scope of application is limited. This right only applies when the lawful basis for processing this information is consent (Article 5(1)(d)) or the performance of a contract (Article 5(1)(c)) and when carrying out the processing by automated means.

Conversely, it does not apply to processing carried out in the performance of a task in the public interest based on law (Article 5(1)(a)) and the other grounds for lawfulness in Article 5. Since Article 5(1)(a) is the most common ground for lawfulness of processing in the EUIs, the **scope of the right to data portability is rather narrow in the EUIs**.

It is possible that your EUI does not carry out any processing operations to which the right to portability applies. **Where this right does not apply in the first place, there can logically be no need to restrict it**.

When drafting their internal rules, EUIs should check if they (1) carry out processing operations to which the right to data portability applies and (2) whether there is a justified need under Article 25(1) to restrict this right. If the answer to either question is 'no', then do not include the possibility to restrict the right to portability in your internal rules, because it is not applicable anyway."

3.7.2. Findings

All EUIs had implemented the recommendation.

3.7.3. Recommendations / conclusions

None.

3.8. "Data protection notice" instead of "privacy statement"

One EUI reacted to the respective EDPS recommendation by arguing that they had used the term "privacy statement" for a long time and that a sudden change of terminology could cause internal and external confusion.

> *"Regarding this recommendation it was stressed that the term "privacy statement" had been used for a long time at (EUI) and was well-established among staff members and also on our websites and records page. I explained that changing the terminology which we used for the general public, our stakeholders, contractors and internal staff members would cause confusion. Moreover, as the Regulation itself does not provide a special terminology in its Art 16 there seemed to be room for flexibility. Also staff members of the EDPS had used themselves the term "privacy statement" on several occasion in slides presented during DPO meetings. As the benefits of the well-established term "privacy statement" for (EUI) were evident, this terminology was kept also in the internal rules so as not to run the risk of causing internal and external confusion due to sudden change of terminology."*

However, the very objective of the EDPS recommendation is to avoid confusion.

Privacy and data protection in EU law are **two separate fundamental rights under the Charter** of Fundamental Rights of the European Union[14] (Article 7 and Article 8 respectively) and they are, consequently, not the same thing[15].

Data protection (not privacy) is the term referred to by Article 16 TFEU[16] ("Everyone has the right to the protection of personal data concerning them"), which in turn is the regulatory legal basis for the Regulation. Article 16 of the Regulation consequently does not have to use any explicit data protection terminology in order to presuppose the existence of a *data protection* notice / statement (as opposed to a privacy notice / statement).

For EUIs operating under the Regulation and on the basis of EU law, data protection notices are exactly that: *data protection* notices (or *data protection* statements, whichever term you prefer).

---

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[15] *If you want to know more, try Juliane Kokott and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, 2013, Vol. 3, No. 4, pp. 222-228, https://academic.oup.com/idpl/article/3/4/222/727206. For the origins of privacy, please see Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, Harvard Law Review Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220, https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents*

[16] Treaty on the Functioning of the European Union.

4. Application of Internal Rules in practice

4.1. Methodology

In phase a) of the audit, DPOs were invited – in cooperation with the staff member(s) responsible on behalf of the controller – to provide replies (**self-assessment**) by filling in a checklist and provide a copy of the decision taken (with the name of the data subject and any other identifiers blackened out).

During phase b) of the audit, the team leader assessed the decision using the criteria contained in the **checklist** (**Annex 2**), taking into account the pieces of evidence submitted as well as the self-assessment provided. The audit results below are thus **not the result of examining individual decisions in detail**, but of assessing their compliance with the main recommendations resulting from EDPS Guidance as outlined in the checklist.

4.2. Findings

In a total of 28 instances, EUIs never actually applied their IR so far, neither in restricting access under Article 17 of the Regulation nor by restricting any other data subject right.

Only in 14 instances, EUIs had applied their IR in practice and provided the EDPS with respective evidence. The number of cases in which EUIs had implemented restrictions using their IR varies significantly between once (four EUIs), twice (three EUIs), four times (one EUIs), 10 times (one EUI), 14 times (one EUI), around 20 (two EUIs), 160 (one EUI) and 272 (one EUI).

In six of these **14 cases, EUIs had not dealt with any restriction of the right of access** under Article 17 of the Regulation. Five EUIs only dealt with one restriction decision, one EUI with six, another one with nine and one EUI with 22.

For the **eight instances involving restrictions to the right of access under Article 17** of the Regulation, during phase b) of the audit, the team leader assessed the decision using the criteria contained in the checklist, taking into account the pieces of evidence submitted as well as the self-assessment provided.

4.2.1. Necessity and proportionality test

On the basis of the IR and for accountability purposes, the data controller should draft a 'proportionality and necessity test' which assesses the need for the restriction. This note should specify which rights are being restricted as well as the reasons and the duration of the restriction. As reflected in the EDPS Guidance, such necessity and proportionality test on the need for restriction should be performed verifying the following elements:

- restriction provided for by law,
- respects the essence of the rights,
- genuinely meets objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others

Example: "An explanation is given about the need of safeguarding the freedoms of others (i.e. the need to protect witnesses)."

- necessary (no alternative equally efficient means to achieve objective)

Example (investigation): "The names of the persons would be known by the data subject in a professional capacity. This is a necessary measure to protect them."

- proportional

Example (medical service, indirect access): "Access to the file is provided; restriction only concerns direct access, only in certain cases and only for part of the medical file. The only aim of the restriction is to avoid risk for data subject's health."

With one exception, there were **no irregularities found regarding the necessity and proportionality tests** conducted by the EUIs. In the exceptional case, necessity and proportionality considerations were only present in the letter sent to the data subject concerned, not in a separate internal note. Since Article 25(6) of the Regulation only requires that the data subject be informed of "the principal reasons on which the application of the restriction is based", EUIs are not obliged to inform the data subjects of the details of the necessity and proportionality tests. However, should EUIs find it acceptable to do so in the specific circumstances of the case concerned, such a letter to the data subject can replace an internal note. Nonetheless, where the EUI is not able or willing to disclose all of the relevant details of such tests, a separate internal note should be drafted in order to ensure that the tests are documented in their entirety.

The above outcome regarding the necessity and proportionality tests was achieved despite the fact that the **involvement of the DPO** was not, in all cases, mandatory under the relevant IR (see above section 3.1) nor ensured in practice (see below section 4.2.6.). However, the very limited number of EUIs having so far implemented their IR in practice (**eight instances only) might not be very representative** of the overall number of EUIs in general. This should thus not be construed as indicating that an involvement of the DPO in the necessity and proportionality assessment is not beneficial or that it should not be an element of the IR.

4.2.2. Information to data subjects

Data subjects should be informed using a general data protection notice, which includes information on potential restrictions. With one exception, data subjects concerned had been individually informed in the cases examined using a general data protection notice, which included information on potential restrictions.

Example: "No general data protection notice was provided in this case as this case concerns a single individual. However, data subjects are informed regarding potential restrictions through a link to the EUI internal rules on restrictions provided on the EUI corporate website in the page dedicated to protection of personal data." The information on the EUI's corporate website reads: "Restrictions to data subject rights might apply in accordance to the internal rules concerning restrictions of certain rights of data subjects (link provided)."

In the above case, the data subject was not individually informed and the link to the existing information was not provided. As a consequence, the data subject was also unaware of the right to lodge a complaint with the EDPS (see Article 25(6) of the Regulation).

4.2.3. Decided on a case-by-case basis

Restrictions must be decided on a case-by-case basis only. There was no indication of blanket measures for any of the cases examined; all evidence provided contained more than generalities and illustrated that considerations regarded the specific case at hand.

4.2.4. Restriction to the least extent possible

In all cases examined, the decision restricted the data subject rights to the least extent possible, thus applying a 'restriction within the restriction' as regards the rights and the extent of the restriction.

> *Example: "Only minimal restrictions applied for a minimal duration (during the duration of the admin. inquiry) to safeguard the investigation and the rights and freedoms of others (especially witnesses)."*

4.2.5. Temporary nature

In most cases examined, the restriction had been temporary and had already been lifted - or will be lifted if the underlying reasoning for its existence no longer applies. In all other cases, valid justifications were brought forward to explain why a certain restriction will need to remain in place indefinitely.

> *Example (protection of a witness in an investigation): "The reasoning for the existence of the restriction will not cease to exist, as there will be a persistent need to protect the personal data of third parties (i.e. the witnesses)."*

4.2.6. Involvement of the DPO

In most, but not all instances, the DPO had been consulted (the controller should involve the DPO throughout the procedure and document this consultation, see sections 3.1 and 4.2.1. above). In one instance (medical service, indirect access was granted), the EUI could justify why the DPO was only informed once the decision to restrict a data subject´s right had been taken.

> *Example (medical service, indirect access): "Restriction under ... Decision... depends on the medical assessment. DPO is informed of the restrictions."*

4.2.7. Documentation of the restriction

In all eight instances examined, the elements justifying the decisions to restrict data subjects´ rights had been documented for accountability purposes.

> *Example: "The EUI uses a Controller Restriction Note, which serves as documentation for accountability purposes. A separate Annex template has been developed "Overview on personal data involved in the investigation". This Annex provides a description of:*
> *1. Reasons (motivated grounds)*
> *2. Objective of the activity (investigation)*
> *3. Number of individuals involved*
> *4. Categories of personal data*

5. Period concerned
6. Means of investigation
7. Confirmation and description of the assessment of the necessity and proportionality and of the definition of the period for restriction and its potential revision."

4.2.8. Monitoring

In most instances examined, restrictions had been monitored on a regular basis. However, in one case, the EUI concerned presented reasons for not subjecting the decision to regular review (see also above, section 3.2.):

"Due to the nature of the restriction, that in the case concerned only refers to the name of other persons, under no circumstances the reasoning for its existence would cease to apply. Therefore, (EUI) does not conduct a regular monitoring of these cases."

4.3. Recommendations / conclusions

Given the **small number of actual decisions** restricting the right to access under Article 17 of the Regulation (eight instances) or any other data subjects' rights, general conclusions are difficult to draw. Given the share of complaints regarding restriction of access under Article 17 of the Regulation (roughly one third over past years) and the number of complaints received by the EDPS in 2020 (40+ admissible complaints), this small number is somewhat surprising.

EUIs should ensure, including by appropriate training, that requests under Article 17 of the Regulation are recognised and dealt with as such, and DPOs should ensure that they are informed well before any decision is actually taken.

The **documented involvement of the DPO** (see section 3.1 above), in particular in the necessity and proportionality assessment **is beneficial** and, for proper implementation, should be an element regulated by the IR. The welcome absence of irregularities regarding the necessity and proportionality tests in practice even without the involvement of certain DPOs (see above section 4.2.1.) should not be construed as indicating the opposite.

Annex 1

1. European Union Agency for the Cooperation of Energy Regulators (ACER)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020Q0423%2801%29
2. Body of European Regulators for Electronic Communications (BEREC)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0424(01)&from=EN
3. European Union Agency for Law Enforcement Training (Cepol)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019Q1111(01)&from=EN
4. Community Plant Variety Office (CPVO)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0810(01)&from=EN
5. Court of Justice of the European Union (CJEU)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.261.01.0097.01.ENG
6. European Commission (EC)	Case 2020-0225 (SG) concerns derogations under Article 25(4) of the Regulation and was dropped from the scope of this audit.
a) COMP	EUR-Lex - 32018D1927 - EN - EUR-Lex (europa.eu)
b) TRADE FDI	EUR-Lex - 32020D1502 - EN - EUR-Lex (europa.eu)
c) TRADE TDI	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D1996&from=EN
d) IAS	EUR-Lex - 32018D1961 - EN - EUR-Lex (europa.eu)
e) HR IDOC	EUR-Lex - 32019D0165 - EN - EUR-Lex (europa.eu)
f) HR D (medical)	EUR-Lex - 32019D0154 - EN - EUR-Lex (europa.eu)
7. European External Action Service (EEAS)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019Q1031(01)&from=EN
8. European Data Protection Supervisor (EDPS)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019Q0410(01)&from=EN
9. European Agency for Safety and Health at Work (OSHA)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020Q0831(01)
10. European Anti-Fraud Office (OLAF)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018D1962&from=EN
11. European Aviation Safety Agency (EASA)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021Q0506(01)&from=EN
12. European Asylum Support Office (EASO)	EUR-Lex - 32020Q0827(01) - EN - EUR-Lex (europa.eu)
13. European Banking Authority (EBA)	EUR-Lex - 32021Q0525(01) - EN - EUR-Lex (europa.eu)
14. European Centre for the Development of Vocational Training (Cedefop)	http://data.europa.eu/eli/dec/2020/1204/oj
15. European Court of Auditors	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021Q0622%2801%29 (published 22 June 2021)
16. European Centre for Disease Prevention and Control (ECDC)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0331(01)&from=EN

17. European Chemicals Agency (ECHA)	EUR-Lex - 32019Q0724(01) - EN - EUR-Lex (europa.eu)
18. European Defence Agency (EDA)	EUR-Lex - 32020Q0407(01) - EN - EUR-Lex (europa.eu)
19. European Fisheries Control Agency (EFCA)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0803(01)&from=EN
20. European Food Safety Authority (EFSA)	EUR-Lex - 32019Q1025(01) - EN - EUR-Lex (europa.eu)
21. European Foundation for the Improvement of Living and Working Conditions (EUROFOUND)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020Q0316%2801%29
22. European Investment Bank (EIB)	eib_decision_on_the_processing_of_personal_data_en.pdf Internal rules restricting the rights of individuals by OCCO and IG/IN Internal rules restricting the rights of individuals by Personnel
23. European Investment Fund (EIF)	EUR-Lex - 32020Q0722(01) - EN - EUR-Lex (europa.eu)
24. European Insurance and Occupational Pensions Authority (EIOPA)	EUR-Lex - 32019Q0826(01) - EN - EUR-Lex (europa.eu)
25. European Joint Undertaking for ITER and the Development of Fusion Energy (F4E)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:037:FULL&from=ES#page=20
26. European Maritime Safety Agency (EMSA)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0706(01)&from=EN
27. European Medicines Agency (EMA)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.209.01.0019.01.ENG&toc=OJ:L:2019:209:TOC
28. European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	EUR-Lex - 32020Q0116(01) - EN - EUR-Lex (europa.eu)
29. European Union Agency for Cybersecurity (ENISA)	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32020Q0210(01)
30. European Ombudsman (EO)	https://www.ombudsman.europa.eu/en/document/en/141577
31. European Parliament (EP)	EUR-Lex - 32019D0802(01) - EN - EUR-Lex (europa.eu)
32. European Securities and Markets Authority (ESMA)	https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1575129513769&uri=CELEX:32019Q1125(01)
33. European Police Office (EUROPOL)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0810(02)&from=EN
34. Fundamental Rights Agency (FRA)	https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A32019Q1104%2801%29
35. European Union Intellectual Property Office (EUIPO)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020Q0327(01)&from=EN
36. The European Union's Judicial Cooperation Unit (EUROJUST)	EUR-Lex - 32020Q0902(01) - EN - EUR-Lex (europa.eu)
37. Single Resolution Board (SRB)	SRB_ES_2019_34_internal security incident investigations SRB_ES_2019_33_protecting the dignity and preventing harassment

	SRB_ES_2019_32_admin inquires_disciplinary proceedings_investigations

Annex 2

In phase a) of the audit, DPOs were invited – in cooperation with the staff member(s) responsible on behalf of the controller – to provide replies (**self-assessment**) by filling in the checklist below and provide a copy of the decision taken (with the name of the data subject and any other identifiers blackened out). During phase b) of the audit, the team leader verified whether the decision identified was in line with the checklist and evaluated the pieces of evidence submitted as well as the self-assessment provided.

Checklist on the application of a restriction under Article 25 in a concrete case

	Criterion	**Reference/evidence/citation of Internal Rules (IR)**	**Assessment (traffic lights) / comments**
1.	A necessity and proportionality test on the need for restriction has been performed (a-e);		
a.	Restriction provided for by law,		
b.	respects the essence of the rights		
c.	genuinely meets objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others		
d.	necessary (no alternative equally efficient means to achieve objective), see also section 4 below)		
e.	proportional		
2.	Data subjects have been informed using a general data protection notice which includes information on potential restrictions;		
3.	Restriction was decided on a case-by-case basis only (no indication of blanket measure, considerations regard specific case)		
4.	Restriction to the least extent possible (a 'restriction within the restriction' should apply as regards the rights and the extent of the restriction)		
5.	Restriction is temporary and will lifted if the underlying reasoning for its existence no longer applies		
6.	The DPO was consulted before and during the restriction (the controller should involve the DPO throughout the procedure and document this consultation)		
7.	Restriction has been documented for accountability purposes		
8.	Restriction is being monitored on a regular basis.		

Annex 3

STANDARD OPERATING PROCEDURE

Control Page

idm@F4E ref:	**...**	**Date:**
Document title:	**Access Request to Personal Data (ref.)**	
Areas and functions		
Version Responsible:	... (DPO)	
Document Owner:	... (DPO)	
Process Group and Context	Organisation and Management System; Internal Governance	
Function(s) concerned	- Controller - Process Owners - DP Coordinators (support to Process Owner) - Data Protection Officer (DPO), for advice, coordination and register - ICT/DMO, for advice support on security measures and document management	

Purpose

This document describes the procedure to follow in case a data subject requests access to his/her personal data in accordance with Regulation (EU) 2018/1725 [1].

Scope

This process is applicable to any access request to personal data for which F4E is the Controller.

Table of contents

Reference documents

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council 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 (EUDPR)

[2] Decision of the Director nomination of DPO final 2 (223K2A)

[3] F4E Net - Register of Privacy Notices and Records

[4] Personal Data Access Request (2KK3WF)

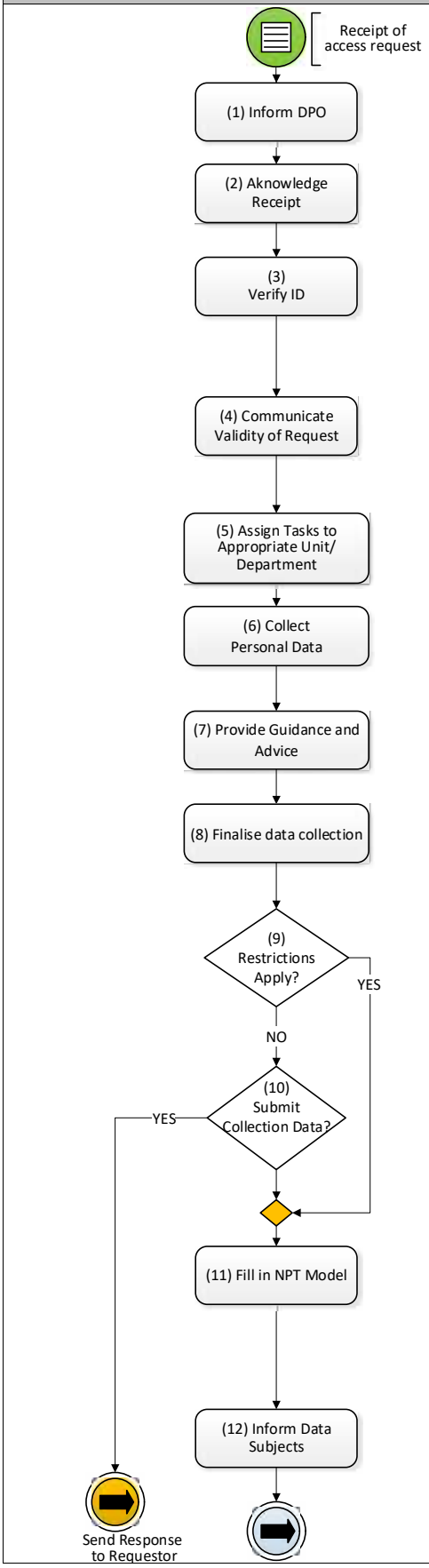
[5] Decision of the Governing Board of Fusion for Energy of 9 December 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of fusion for energy

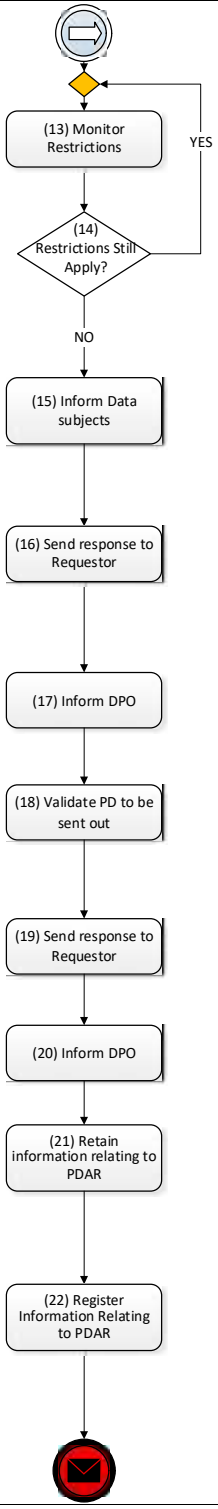
Definitions/ Abbreviations	Refer to F4E Acronyms, Glossary and F4E Roles in the Manual for more information
Controller	Means the organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controllers have the prominent role in the correct application of the data protection requirements as they determine the purposes and means of the processing of personal data in their activity area. In particular, the Controllers' duties are to ensure the lawfulness of the processing of data carried out by the members of their staff (the Process Owners), ensure the confidentiality and the security of the processing, inform the Data Subjects of their rights and ensure that their rights can be properly exercised. The Controllers need to include the data protection measures in the processes/policies of the processing operations. The Controller must co-operate with the Data Protection Officer (DPO) and may consult him or her for an opinion on any data protection related question. The Controller must notify the processing operation prior to its implementation to the DPO. In the implementation of their data protection duties, the Controllers are supported by the Coordinators specifically nominated by them for this purpose.
DP Coordinator (DPC)	A person in the respective Unit/Department to assist the Process Owner in the exercise of the data protection duties. The Coordinator in particular provides advice and coordinates the proper implementation of the data protection requirements in the Unit/Department, ensures that data protection requirements are properly addressed in the relevant processes and prepares (with the Process Owner) the documentation requested for each of the processing operations. The Coordinator liaises and co-operates with the DPO and represents the Controller in the Data Protection Network.
Data Protection Officer (DPO)	The DPO ensures compliance of F4E with the Regulation in force; controls and advises on the lawfulness of the processing of the personal data. The DPO maintains a register of all records and privacy notices for all F4E processes and controls their correct publication or communication to data subjects. In special cases, the DPO shall consult the European Data Protection Supervisor (EDPS) on the lawfulness of the processing operations. In crucial circumstances, he may investigate matters and incidents on request or on his own initiative. The DPO chairs the Data Protection Network composed of the Coordinators.
Data Subject (DS)	Natural person whose personal data are processed.
European Data Protection Supervisor (EDPS)	An independent supervisory authority established in accordance with Regulation (EU) 2018/1725. The EDPS' mission is to ensure that the fundamental rights and freedoms of individuals - in particular their privacy - are respected when the EU institutions and bodies (including F4E) process personal data. The EDPS is also responsible for advising the EU institutions and bodies on all matters relating to the processing of personal data. He may inspect the EU institutions and bodies on their compliance with the data protection requirements at any time.
Personal Data (PD)	Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data processed at F4E: passport, CV, appraisal of a person's work, e-mail address, signature, etc.
PDAR	Personal Data Access Request
Process Owner (PO)	The Process Owners act as Controller for each of the personal data processing they are in charge of. Example: in case of personal data processed for recruitment the Controller is the Human Resources Unit and the Process Owner is the staff member responsible for the Recruitment procedure.

Responsibilities

F4E Staff member	- Notifies DPO and Process Owner of the reception of an access request. Access Requests are usually addressed to either the Controller's functional mailbox (fmb) appearing in the Privacy Notices to the F4E Director or to the DPO. But any staff member may receive it.
Process Owner, with the support of the DP Coordinator	Sends an e-mail to requestor acknowledging receipt of request. Verifies identity of the requestor. Collects all the personal data processed by the Unit/Department. Seeks guidance with DPO on which document can be sent. - If restrictions apply (application of Article 25): o Liaise with DPO all through the period during which the restrictions applies, and documents consultation with DPO; o Monitors the necessity of the restrictions; o Informs data subject when the restriction no longer applies (when sending the data requested). Sends the personal data by encrypted means. - Informs the DPO of actions taken (categories of data sent and date of dispatch). Retains information relating to PDAR.
DPO	- Identifies Controllers and informs Coordinator(s) in respective Unit(s)/ Department(s) - Provides guidance and advice to DP Coordinators and Process Owners, in particular with Article 25 has to be applied - Validates PD to be sent out - Registers information relating to PDAR

1. Procedure Flow

Activity	#	Resp.	Guidance
	**0**		**Trigger:** Receipt of access request Go-to 1. Inform DPO.
	1	Staff Member	**Inform DPO** Inform DPO that a personal data access request was received. Go-to 2. Acknowledge Receipt.
	2	PO	**Acknowledge Receipt** Without undue delay, send an e-mail to requestor acknowledging receipt of request. Go-to 3. Verify ID.
	3	PO	**Verify ID** Verify ID of requestor and validity of request. If requestor is: - the data subject – ask for a valid form of ID - a third party - request for written confirmation that the requestor is authorised to act on behalf of the data subject (e.g. power of attorney). Go-to 4. Communicate Validity of Request.
	4	DPO	**Communicate Validity of Request** Once the request is considered valid, inform requestor of the validity of the request and the deadline by which the Controller(s) will provide the PD processed by F4E. Go-to 5. Assign Tasks to Appropriate Unit/ Department.
	5	DPO	**Assign Tasks to Appropriate Unit/ Department** Identify the Unit(s)/ Department(s) concerned (Data Protection Coordinator) and assign tasks in accordance with the scope of the request. Go-to 6. Collect Personal Data.
	6	PO	**Collect Personal Data** Fill in the PDAR template. *Template*: Go-to 7. Provide Guidance and Advice.
	7	DPO	**Provide Guidance and Advice** Provide support and guidance to the DP Coordinators and Process Owners (meetings, e-mails exchanges, guidance notes, etc.). Go-to 8. Finalise Data Collection.
	8	PO	**Finalise Data Collection** Finalise PDAR table and assess possible need for restriction under Article 25. Go-to 9. Gate: 'Restrictions Apply?'
	9	PO	**Gate: 'Restrictions Apply?'** Do restrictions under Art. 25 apply? YES: Restrictions apply. Go to 11. Fill In Necessity And Proportionality Test Model. NO: Restrictions do not apply. Go to 10. Gate: 'Submit Collected Data?'
	10	DPO	**Gate: 'Submit Collected Data?'** YES: Go to 16. Send Response to Requestor. NO: Go to 11. Gate: 'Fill In Necessity and Proportionality Test Model (NPT Model)'
	11	PO	**Fill In Necessity and Proportionality Test Model (NPT Model)** Draft an internal and confidential note, following the template. *Template*: Internal note on a concrete restriction - Necessity and proportionality test model (2RNT3F) . Go-to 12. Inform Data Subjects.
	12	PO	**Inform Data Subjects** Inform data subjects of the main reasons on which the application of the restrictions are based on and their right to lodge a complaint, unless recommended otherwise by the DPO. Go-to 13. Monitor Restrictions.
	--		Continue procedure on next page.

<table>
<tr><th>Activity</th><th>#</th><th>Resp.</th><th>Guidance</th></tr>
<tr><td rowspan="11"> 
</td><td>--</td><td colspan="2">Continue procedure.</td></tr>
<tr><td>13</td><td>PO</td><td>Monitor Restrictions
Monitor restrictions according to milestones set in the necessity and proportionality model.
Go-to 14. Gate: ‘Restrictions Still Apply?’</td></tr>
<tr><td>14</td><td>PO</td><td>Gate: ‘Restrictions Still Apply?’
In consultation with the DPO, assess the need for the restriction.
Do restrictions still apply?<table><tr><td>YES</td><td>Go-to 13. Monitor Restrictions.</td></tr><tr><td>NO</td><td>Go-to 15: Inform Data Subjects.</td></tr></table></td></tr>
<tr><td>15</td><td>PO</td><td>Inform Data Subjects
In consultation with the DPO, inform data subjects that the restrictions are no longer applicable.
Go to 16. Send Response to Requestor.</td></tr>
<tr><td>16</td><td>DP Controller</td><td>Send Response to Requestor
Within one month of receipt of the request, send the PD processed in respective Dept./ Unit by encrypted means to the requestor.
The Data Subject is normally entitled to a copy of the information in permanent form.
Go-to 17. Inform DPO.</td></tr>
<tr><td>17</td><td>PO</td><td>Inform DPO
Inform DPO of Action Taken.
Go-to 18. Validate PD to be Sent Out</td></tr>
<tr><td>18</td><td>DPO</td><td>Validate PD to be Sent Out
Screen the data collected by the Coordinators based on the completed PDAR and provide final guidance on PD to be released to the Requestor.
Go-to 19. Send Response to Requestor.</td></tr>
<tr><td>19</td><td>DP Controller</td><td>Send Response to Requestor
Within one month of receipt of the request, send the PD processed in respective Dept./Unit by encrypted means to the requestor.
The Data Subject is normally entitled to a copy of the information in permanent form.
Go-to 20. Inform DPO.</td></tr>
<tr><td>20</td><td>PO</td><td>Inform DPO
Inform the DPO of the categories of data sent to the Data Subject/ requestor and date of dispatch, without undue delay.
Go-to 21. Retain Information Relating to PDAR.</td></tr>
<tr><td>21</td><td>DP Controller</td><td>Retain Information Relating to PDAR
Keep a record of the documents sent to the requestor, in case any follow up actions are required.
Go-to 22. Register Information Relating to PDAR.</td></tr>
<tr><td>22</td><td>DPO</td><td>Register Information Relating to PDAR
Keep a register of messages sent out by respective Controllers to the requestor (note: DPO does not have access to the encrypted personal data enclosed in these messages).</td></tr>
<tr><td>--</td><td colspan="2">Procedure ends</td></tr>
</table>

Template for Restriction of Data Subject Rights

The parts highlighted in yellow should be either adapted or removed in the final version

Consultation of the Data Protection Officer on [add date].

The controller, on the basis of the EUDPR[17], in particular its Article 25, and the corresponding F4E internal rules published in the Official Journal on 9 December 2019, has decided to restrict the following data subjects right[s]:

- Restricted rights: [specify the rights from Articles 14 to 22, 35, and 36 of Regulation No 2018/1725, as well as its Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22],
- Persons concerned [specify persons concerned]
- Categories of data concerned [specify categories of personal data].

[The duration of the restriction is] [indicate a period of max. 6 months]. / [The restriction is being renewed in consultation with the Data Protection Officer for a period of [max.6 months] corresponding to a total period of [indicate total period of restriction including present renewal] which started on [indicate date].

By [confidential/restricted] decision of …. dated [add date], F4E [opened an inquiry/referred a case to OLAF/ referred a case to IDOC/opened an internal investigation] regarding [add person/case].

The main purpose for the processing of personal data is: [insert a short description].

The restriction is necessary for the following reasons: [explain briefly the background].

The legal basis for the restriction is: [indicate one or several reason(s) listed in Article 25(1) of Regulation No 2018/1725 such as: national security, public security, defence of the Member States, prevention, investigation, etc.].

The restriction is considered to be proportional for the following reasons: [weigh restriction vs. the risks to the rights and freedoms of data subjects].

[Name of staff member responsible on behalf of Controller]

Signed electronically

[17] *Regulation No 2018/1725 of the European Parliament and of the Council 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.*