What happened to the Risk Based Approach to Data Transfers?

How the EDPB is rewriting the GDPR

The following is a guest post to the FPF blog from Lokke Moerel, Professor of Global ICT Law at Tilburg University and a lawyer with Morrison & Foerster (Brussels).

The guest blog reflects the opinion of the author only. Guest blog posts do not necessarily reflect the views of FPF.

Prof. Lokke Moerel

1. Introduction

In my earlier FPF guest blog on the *geopolitics of trans-Atlantic data transfers*, I flagged that following Schrems II companies increasingly find themselves in catch-22. Frustrations are running high, as companies work towards *Schrems II* compliance by executing measures to mitigate the risk that U.S. government entities can access their data. Yet, EU data protection authorities (**DPAs**) continue to block their way. The DPAs increasingly adopt an absolutist approach, whereby mitigating measures are disregarded irrespective of the actual risk for data protection after transfer, triggering a debate on what happened to the risk-based approach of the GDPR (**RBA**). This has come to the fore in recent decisions of the DPAs as to the data transfers in the context of the use of Google Analytics. The Austrian DPA kicked things off by issuing a decision in a complaint of nyob against i.a. Google (**GA decision**).[1] In this decision, the Austrian DPA *explicitly* discards the applicability of the RBA as far as the data transfer provisions of the GDPR are concerned. In a Q&A issued by the CNIL concerning the use of Google Analytics, the CNIL also indicated that the RBA cannot be applied to data transfers.[2]

This is noteworthy, as in legal literature, it is generally assumed that the RBA is incorporated in the 'accountability principle' of Article 24 GDPR and that this principle has a horizontal application throughout the GDPR and therefore also applies to the data transfer requirements.[3]

.

[1] https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf. See for English translation: Standarderledigung Bescheid (noyb.eu)

[2] The CNIL also issued a Q&A concerning the use of Google Analytics: https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics
The last question of the Q&A refers to the use of RBA by controllers by taking into account the likelihood of data access requests. The CNIL indicates that the RBA approach cannot be applied and explains that as long as the access to the transferred data is possible and the safeguards governing the issuance of requests for access to data do not guarantee a level substantially equivalent to the one guaranteed in the EU, it is necessary to take additional technical measures to make such access impossible or ineffective.

[3] See, specifically on the applicability of the RBA to data transfer requirements after the Schrems II judgement: Paul Breitbarth, "A Risk-Based Approach to International Data Transfers," EDPL, 2021, p. 547; Christopher Kuner, 'Schrems II Re-Examined' (VerfBlog, August 25, 2020) , https://verfassungsblog.de/schrems-ii-re-examined/; and

In this light, it is high time for an in-depth assessment whether, and if so, to what extent, the GDPR introduced the RBA, and specifically whether the RBA also applies to the data transfer requirements of Chapter V of the GDPR.

The conclusion will indeed be that the accountability requirement of Article 24 GDPR incorporates the RBA for all obligations of the controller in the GDPR. Where the transfer rules are stated as obligations of the controller (rather than as absolute principles), the RBA of Article 24 therefore applies. Other than the DPAs assume, this is not contradicted by the ECJ in Schrems II nor by the EDPB recommendations on additional measures following the Schrems II judgement. We will however also see that the EDPB is trying to rewrite the GDPR, by applying the accountability principle of Article 5(2) GDPR (which does **not** include the RBA), rather than the accountability principle of Article 24, which does. By taking this position, the EDPB basically pushes its own version of the accountability principle as proposed at the time for revision of the Directive, which was, however, ultimately not adopted by EU regulators in the GDPR.

2. Reasoning Austrian DPA in GA decision

In the GA decision, the Austrian DPA rejected Google's arguments that a RBA should be taken when assessing the impact of the data transfers in the context of Google Analytics and that the Austrian DPA applies too strict a standard when considering that the mere possibility of access is relevant and not the actual risk of U.S. public authorities accessing the data.

Specifically, the DPA reasoned that such RBA cannot be derived from the wording of Art. 44 GDPR. See the decision point D.4 (underlining by Austrian DPA in the original decision):

> **"Art. 44 GDPR - General principles of data transmission**
> "Any transfer of personal data already processed or to be processed after their transfer to a third country or an international organization shall only be allowed if the controller and the processor comply with the conditions laid down in this Chapter and with the other provisions of this Regulation, including any onward transfer of personal data from that third country or international organization to another third country or international organization. All provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Regulation is not undermined."
>
> On the contrary, it can be deduced from the wording of Art. 44 GDPR that for every data transfer to a third country (or to an international organization), it must be ensured that the level of protection guaranteed by the GDPR is not undermined.
>
> The success of a complaint of a violation of Art. 44 GDPR therefore does not depend on whether a certain "minimum risk" is present or whether U.S. intelligence services have actually accessed data. According to the wording of this provision, a violation of Art. 44 GDPR already exists if personal data are transferred to a third country without an adequate level of protection.

Christopher Kuner, Lee Bygrave and Christopher Docksey, The EU General Data Protection Regulation: A Commentary. Update of Selected Articles. Oxford University Press, 2021, p. 113. Other authors discuss the RBA of the GDPR, but not specifically in the context of data transfers and the ECJ judgement in the Schrems II case.

> In connection with those provisions of the GDPR where a risk-based approach is actually to be followed ("the higher the processing risk, the more measures are to be implemented"), the legislator has also explicitly and without doubt standardized this. For example, the risk-based approach is provided for in Art. 24(1) and (2), Art. 25(1), Art. 30(5), Art. 32(1) and (2), Art. 34(1), Art. 35(1) and (3) or Art. 37(1)(b) and (c) GDPR. Since the legislator has standardized a risk-based approach in numerous places in the GDPR, but not in connection with the requirements of Art. 44 GDPR, it cannot be assumed that the legislator merely "overlooked" this; an analogous application of the risk-based approach to Art. 44 GDPR is therefore excluded."

The Austrian DPA further rejected the arguments of Google that that the RBA was confirmed by the European Court of Justice (**ECJ**) in the Schrems II judgement.[4] According to the Austrian DPA:

> "In its analysis of the legal situation in the United States and the validity of the EU-U.S. adequacy decision precisely did not assume a risk-based approach in Chapter V of the GDPR. In fact, such a risk-based approach is not mentioned in the said judgment.
>
> The second respondent apparently derives a risk-based approach from the phrase "adequate level of data protection" used by the ECJ. This cannot be accepted, as the ECJ used this wording with reference to Recital 108 of the GDPR. It is clear from Recital 108 of the GDPR that "adequate level of data protection" means that the rights of data subjects are to be respected in an appropriate manner.
>
> With regard to the legal situation in the United States, the ECJ has assumed that, due to the disproportionate access possibilities of U.S. authorities, an "adequate level of data protection" cannot be assumed, which is why it ultimately declared the EU-U.S. adequacy decision invalid.
>
> The ECJ expressly did not consider the fact that the obligations to which a Privacy Shield-certified company from the U.S. is subject may be adequate after all in individual cases (for example, because the certified company merely receives non-sensitive or non-criminal personal data)"

The DPA also rejected Google's arguments that the RBA can be considered included in the EC Implementing Decision (EU) 2021/914, which adopted new standard contractual clauses, as well as that the EDPB's Recommendations 01/2020 on measures to complement transfer tools to ensure the level of protection of personal data[5] under EU law.

The Austrian DPA further states that the GDPR:

> "Unlike Chapter V - see below - Art. 5(2) in conjunction with Art. 24(1) GDPR now actually take a risk based approach. The higher the risk associated with the data processing, the higher the standard for the evidence to be submitted in order to prove compliance with the GDPR."

[4] Case C-311/18 *Data Protection Commissioner v Facebook Ireland* Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559 : CURIA - Case information (europa.eu).
[5] edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu).

3. Questions of law to be investigated

Based on the GA decision, there are a number of questions of law to be investigated:

1) Does the RBA apply to the accountability requirements in Article 24 only, in the sense that the **standard of evidence** (i.e., the required accountability measures, like policies, training requirements, etc.) scales with the risk of the relevant processing rather than that the RBA applies also to the underlying obligations of the controller set out in other provisions of GDPR?

2) Is the position under 1) supported by the fact that where the EU regulator intended to implement the RBA, this is explicitly expressed in the relevant provisions only? [which seems to be the position of the Austrian DPA]

3) If the position under 1) is not correct, and RBA in Article 24 GDPR must be considered to constitute a horizontal provision applying a RBA also to the underlying obligations of the controller, does the RBA then relate to the obligations of controllers in Chapter IV only, or to all data protection obligations of controllers, including those of Chapter V?

4) Does Article 5(2) indeed take a RBA for the accountability principle? [which seems to be the position of the Austrian DPA]

5) Is the position under 1) confirmed by the ECJ in the Schrems II judgement?

6) Is the position under 1) confirmed by the EDPB Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (**EDPB Recommendations**)?[6]

4. Summary conclusions

Based on an analysis of the wording of the GDPR (see Section 6), the legislative history of the GDPR (see Section 7), the Schrems II judgement (see Section 8) and the EDPB Recommendations (see Section 9) the conclusions are:

- The accountability requirement of Article 24 incorporates the RBA. Article 24 has a horizontal application and the RBA therefore applies not only to the standard of evidence (accountability measures required), but also to the underlying obligations of the controller in the GDPR. Where the transfer rules are stated as obligations of the controller (rather than as absolute principles), the RBA of Article 24 therefore applies.

- The accountability principle of Article 24 does not apply to the general processing principles of Article 5(1). The accountability principle of Article 5(2) applies to the general processing principles only, which do not include the data transfer principles. Article 5(2) does **not** include the RBA.

[6] Ibid.

- The ECJ in Schrems II has raised the bar as to data transfers based on Article 46 (transfers subject to appropriate safeguards), in the sense that when personal data are transferred these require an **essentially equivalent** level of protection (rather than an adequate level), this in reference to the general principle for transfers of Article 44 and the EU Charter of fundamental rights. In the absence of an adequacy decision, the ECJ considers it the **responsibility of the controller** to make a transfer assessment before a transfer can take place on the basis of appropriate safeguards, which also includes an assessment of the laws **and practices** of the country or countries where the data are flowing to (see para. 126: where the ECJ explicitly refers to "the law and practices in force in the third country concerned" and requires "(...) ensuring, **in practice**, **the effective protection** of personal data transferred to the third country concerned."[7] The controller should then take measures to compensate for any lack of data protection by way of appropriate safeguards. The Court does not require that additional safeguards provide a 100% guarantee that access to data by third parties can never occur, but rather that they constitute "effective mechanisms that make it possible, **in practice**, to ensure compliance with the level of protection required by EU law…" (para. 137). Though the ECJ did not explicitly refer to the accountability principle of Article 24, this transfer assessment obligation of the controller seems in line with the RBA of the accountability principle of Article 24.

- The EDPB Recommendations confirm that Schrems II is in line with the accountability principle and that this principle applies also to the data transfer rules. Though the EDPB Recommendations refer to the accountability principle of Article 5(2) GDPR only, the EDPB Recommendations seems to allow for a nominal RBA as to the transfer assessment, this in line with the RBA of Article 24 and Schrems II.

5. Interpretation of Article 5 and 24 GDPR

According to settled case law of the ECJ, the interpretation of a provision of EU law requires that account be taken not only of its wording and the objectives it pursues, but also of its legislative context and the provisions of EU law as a whole. Also the origins of a provision of EU law may provide information relevant to its interpretation.[8]

5.1. Relevant provisions & recitals

"Article 5 GDPR - Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall,

[7] See for a similar reference also para. 158.
[8] ECJ judgment of December 10, 2018, *Wightman and Others*, C-621/18, EU:C:2018:999, paragraph 47 and the case-law cited: CURIA - Case information (europa.eu)

in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Article 24 GDPR - Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Recitals

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

6. Textual analysis

Article 24 is the first provision of Chapter IV (Controller and processor) Section 1 (general obligations). Reviewing the language of Article 24 GDPR, it very much resembles that of Article 25 (Data protection by design and by default) and Article 30 (Security). The heading of Article 24 is "Responsibility of the controller," and the provision starts with the qualifier "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall…." It is not under discussion that this implies the RBA.

The question then is whether the RBA applies to the **standard of evidence** (the accountability measures) or also to the underlying obligations of the controller under the GDPR themselves. The text of Article 24 reads that the controller must "**ensure** and to be able to demonstrate that processing is performed **in accordance with this Regulation**." Where the controller explicitly has to **ensure** compliance taking a RBA, it is difficult to see why the RBA in Article 24 would only apply to level of **standard of evidence** (i.e., to be able to **demonstrate compliance**) and

not to the underlying controller obligations themselves. The obligation further explicitly refers to **all requirements** under the Regulation.

That being said, not all provisions of the GDPR are formulated as obligations of the controller. For example, the general processing principles listed in Article 5(1) are not formulated as obligations of the controller, but as absolute principles. In Article 5(2) it is subsequently provided that "the controller is responsible for, and shall be able to demonstrate compliance with paragraph 1 ("accountability")." Noteworthy here is that this accountability requirement is not in any manner qualified, taking a RBA similar as in Article 24. This seems to mean that the RBA does not apply to the material processing principles (why otherwise include Article 5(2) in the first place; in that case Article 24 GDPR would have been sufficient).

The question then is how does this apply to the data transfer rules of Chapter V? There is no indication whatsoever in the GDPR that the general obligation of the controller of Article 24 would not also apply to obligations of controllers under Chapter V (again Article 24 requires that controllers ensure compliance with **the Regulation**).

Rather, there are indications to the contrary. For example, the privacy-by-design requirements and security requirements (which also incorporate the RBA) remain applicable when transferring data (see explicitly Recital 108). In the same vein, also the accountability principle will be applicable when transferring data (provide the transfer rules are formulated as obligations of the controller rather than in absolute principles).

As the Austrian DPA notes, the general principle for transfers in Article 44 does indeed provide that "any transfer of personal data shall only take place in accordance with the conditions of this Chapter," but (as omitted by the Austrian DPA) this general principle is explicitly made "subject to the other provisions of this Regulation." This is logical, Chapter V on transfers cannot be considered on a standalone basis. The transfer rules aim to ensure that data receives a similar level of protection also after being transferred to a third county that does not provide for an adequate level of protection, **not a higher protection**. This is also expressed in the last sentence of Article 44:

> "All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

Article 46 GDPR (transfers subject to appropriate safeguards) is further formulated not as an absolute principle (like the general processing principles of Article 5(1)), but as an obligation of the controller where it allows data transfers "if the controller (…) has provided appropriate safeguards and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available."

The conclusions seems justified that the obligation of the controller "to provide appropriate safeguards" under Article 46 GDPR are indeed risk based, with the exception of where Article 46(1) provides for the absolute requirements "that enforceable data subject rights and effective legal remedies for data subjects are available."

That the accountability provision of Article 24 and the data transfer rules have overlap and should be considered together, is further supported by the fact that Article 24(3) indicates that 'adherence to approved codes of conduct under Article 40 or approved certification mechanisms under Article 42, may be used as **an element to demonstrate compliance with the obligations of the controller**, which codes and certification mechanisms are also listed in Article 46(2) sub (e) and (f) as means **for controllers to provide 'appropriate safeguards' for data transfers.**

6.1. Conclusions based on textual analysis

Based on a textual analysis of Articles 5, 24 and Chapter V, it seems the answers to the issues are as follows:

1) Does the RBA apply to the accountability requirements in Article 24 only, in the sense that the **standard of evidence** (i.e., the required accountability measures, like policies, training requirements, etc.) scales with the risk of the relevant processing rather than that the RBA applies also to the underlying obligations of the controller set out in other provisions of GDPR;

   A: The accountability requirement of Article 24 has a horizontal application and the RBA applies not only to the standard of evidence, but also to the underlying obligations of the controller in the GDPR.

   The accountability principle of Article 24 does not apply to the general processing principles of Article 5(1). The accountability principle of Article 5(2) applies to the general processing principles, which do not include the data transfer principles. Article 5(2) does not include the RBA.

   Where individuals have absolute rights, these prevail. The rights of individuals are therefore not risk based, but the accountability measures required of the controller to implement these are.

2) Is the position under 1) supported by the fact that where the EU regulator intended to implement the RBA for specific requirements, this is explicitly expressed in the relevant provisions?

   A: No. See previous answer.

3) If the position under 1) is not correct, and RBA in Article 24 GDPR must be considered a horizontal provision applying a RBA also to the underlying requirements, does the RBA then relate to the obligations of controllers in Chapter IV only, or to all data protection obligations of controllers, including those of Chapter V?

   A: The RBA applies to all obligations of the controller under the GDPR. Where the transfer rules are stated as obligations of the controller (rather than as absolute principles), the RBA of Article 24 therefore applies.

4) Does Article 5(2) indeed take a RBA for the accountability principle? [which seems the position of the Austrian DPA]

A: No, the accountability principle in Art. 5(2) does not include the RBA.

As indicated, the provisions of the GDPR can, however, not be taken at face value, but have to be interpreted in light of the legislative history of the GDPR, which here includes its predecessor, the EU Data Protection Directive.

7. Legislative history Article 5 and 24 GDPR

7.1. The EU Data Protection Directive

Historically EU data protection legislation has been "rights-based," and the requirements were to be applied irrespective of the level of risk involved and whether actual harm was created.[9] As the WP29 (the predecessor of the EDPB) put it at the time, the EU data protection legal framework provides for a 'minimum and non-negotiable level of protection for all individuals.'[10] This all the more so since the entry into force of the Treaty on the Functioning of the European Union in 2010, which granted the right to personal data protection the status of a fundamental right of the EU. See Article 8 of the EU Charter (and Article 16(1) of TFEU):

> **Article 8 Protection of Personal Data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Noteworthy is that the protection of data transfers is not among those listed as a fundamental right. The EU transfer rules are not considered to be one of the material processing principles, as the transfer rules are a mechanism to ensure that these material processing principles will be observed, rather than being a fundamental processing principle itself.[11] This being said, the transfer rules are crucial in their own right to guarantee the protection provided by the EU Data

---

[9] See, *Amann v Switzerland* App No 27798/95 (ECtHR, February 16, 2000) §70: in order to determine whether a processing constitutes an interference, the fact that the data subject may 'have been inconvenienced in any way' is irrelevant: AMANN v. SWITZERLAND (coe.int).

[10] Art. 29 WP, 'Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) , (1998), p. 2: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf.

[11] This is evidenced by the fact that in the Directive the EU transfer rules are not included in Chapter II (The General Rules on the Lawfulness of the Processing of Personal Data), but in a separate Chapter IV (Transfer of personal Data to third Countries). For a similar separation of the basic principles and the transfer rules see the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (**Madrid Draft Proposal for International Standards**), as adopted on November 5, 2009 at The International Conference of Data Protection and Privacy Commissioners in Madrid by the participating data protection authorities, to be found at < https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf >, where the transfer rules are included in Section 15 and the basic principles of data protection in Part II.

Protection Directive (**Directive**) and therefor are a key cornerstone of the Directive.[12] This distinction is continued in the GDPR, where the material processing principles are listed in Article 5(1) GDPR (and do not include data transfer requirements) and the data transfer requirements are regulated separately in Chapter V.

7.2. Legislative reform

The Directive did not include an accountability principle and it was only as part of the legislative review of the Directive that this principle was introduced. The main trigger for introducing the accountability principle was that the legislative review of the Directive by the EC showed that there was a widespread lack of compliance with the Directive, in particular also the data transfer requirements, and that the enforcement tools of the DPAs were not sufficient to force compliance.[13] On July 9, 2009, the EC launched a consultation on the EU data protection legal framework. As part of the consultation, the WP29 and EDPS issued a number of opinions, which basically advised the EC to introduce the accountability principle in the revised Directive. The proposals of the WP29 developed somewhat over time, but its lasts stance was basically adopted by the EC in its first proposal for a new Regulation. Below I discuss the relevant opinions of the WP29, to show how the proposals developed, which will be helpful to understand the subsequent changes made to the text as ultimately adopted in the GDPR.

(a) Joint paper "The Future of Privacy" (December 2009)

In December 2009, the WP29 together with the Working Party on Police and Justice (**WPPJ**) issued a joint paper "The Future of Privacy"[14] (**Joint Paper**) in which they expressed the view that the present European legal framework for data protection had not been successful in ensuring that the data protection requirements translate into effective mechanisms that deliver real protection.[15] To improve this situation, the WP29 and the WPPJ proposed to the EC to

[12] See WP 12, Working Document on Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, July 24, 1998 (**WP 12**), at < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf >, where the Working Party 29 lists "six content principles" of which the 6th is: "restrictions on onward transfers - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e., the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive." Since a restriction on onward transfers was at the time missing from Convention 108, the Working Party 29 considered the protection provided by the countries that had at the time ratified Convention 108 was insufficient (see WP 12, at 8). This led to adoption of a transfer rule similar to the Directive in Article 2 of the Additional Protocol to Convention 108.

[13] Rand Europe, Review of the European Data Protection Directive, Technical Report dated May 2009 (**Rand Report**) at < https://www.rand.org/pubs/corporate_pubs/CP1-2009.html >. Other reviews showed similar results: see Douwe Korff, *EC Study on implementation of the Data Protection Directive, Comparative study of national laws*, September 2002, Human Rights Centre University of Essex, at 209, to be found at <http://papers.ssrn.com>, notes that "the powers now vested in the data protection authorities, as currently exercised, have not been able to counter continuing widespread disregard for the data protection laws in the Member States."

[14] WP Contribution on The Future of Privacy, at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf.

[15] ibid. p.2: "[T]he main principles of data protection are still valid despite these important challenges. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice."

include the "principle of accountability" in the revised Directive.[16] With the acknowledgement that "accountability" may have different meanings in different languages and legal systems,[17] the WP29 and WPPJ proceeded with describing the measures which "accountability" requires (rather than focusing on a definition). In short, this principle entails that the controller is required:

(i) to implement appropriate and effective measures to put the **material processing principles** of the Directive into effect;
(ii) to demonstrate these measures to the DPA on its request.

The Joint Paper (para. 80) reflects that the **accountability measures** (rather than the material principles themselves) **should be scalable**: "In any event, the measures expected from data controllers should be scalable and take into consideration the type of company, whether large or small, and of limited liability, the type, nature and amount of the personal data by the controller, among other criteria."

The Joint Paper leaves no doubt that the accountability measures also concern the data transfer rules, for example (see para. 37) the WP29 advises under the heading "Binding Corporate Rules / Accountability," the EC to officially recognize BCRs as appropriate tool to provide adequate safeguards and to define the main substantive and procedural elements of BCRs. The Joint Paper even advises (see para. 39) to include an accountability requirement for onward transfers to controllers in third countries:

> "39. Moreover, from a general point of view, a new provision could be included in the new legislative framework pursuant to which data controllers would remain accountable and responsible for the protection of personal data for which they are controllers, even in the case the data have been transferred to other controllers outside the EU (see on 'accountability' more in general Chapter 6).

(b) WP29 Opinion on the accountability principle (July 2010)

As a follow up to its WP Contribution on The Future of Privacy, the WP29 issued a specific Opinion on the accountability principle,[18] elaborating the implications of the accountability principle in practice. See para 12:

> "One way to induce data controllers to put in place such measures would be by adding an accountability principle in the revised version of the Directive. The expected effects of

---

Also at para. 78: "In practice Article 17 (1) has not been successful in making data protection sufficiently effective in organizations, also due to different approaches taken in the national implementing measures."

[16] ibid. para. 79.

[17] WP Opinion on the principle of accountability: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. para. 21: "The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning – even though defining what exactly accountability means is complex. In general terms though, its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed."

[18] WP Opinion on the principle of accountability: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

> such a provision would include the implementation of internal measures and procedures putting into effect existing data protection principles, ensuring their effectiveness and the obligation to prove this should data protection authorities request it. As further described below, the type of procedures and mechanisms would vary according to the risks represented by the processing and the nature of the data."

The Working Party 29 proposed the following concrete provision:

> "Article X – Implementation of data protection principles
> 1. The controller shall implement appropriate and effective measures to **ensure that the principles and obligations** set out in the Directive are complied with.
> 2. The controller shall **demonstrate compliance** with paragraph 1 to the supervisory authority on its request."

The provision therefore now no longer only specifically refers to the material processing principles but to **all principles and obligations** of the revised Directive. Here again, scalability (which is in fact the RBA) applies to the **accountability measures only** (see para. 53):

> "Therefore, how a controller should ensure the effectiveness of measures will depend on the sensitivity of the data, the amounts of data processed and the particular risks posed by the data processing. Article 29 Working Party guidance on the measures may also include guidance on this aspect."

The WP29 indicates (para. 29) that "The obligation should cover all controllers and all situations, and again confirms that the accountability requirement also extend to the data transfer rules:

> Para 19:
>
> "In addition to the above, the Article 29 Working Party notes that binding corporate rules ("BCRs"), which are used in the context of international data transfers, reflect the accountability principle. Indeed BCRs are codes of practice, which multinational organizations draw up and follow, containing internal measures designed to put data protection principles into effect (such as audit, training programs, network of privacy officers, handling complaint system). Once reviewed by national data protection authorities, BCRs are deemed to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of the same corporate group and that are bound by these corporate rules ex Article 25 and 26.2 of Directive 95/46.
>
> And para. 55:
>
> **"International data transfers**
> Binding corporate rules is an example of a way to implement data protection principles on the basis of the accountability principle. It is a way identified and accepted by the Article 29 Working Party to provide adequate safeguards for transfers outside the European Union."

As to the consequences of compliance with the accountability principle, the WP 29 (at p. 11):

> "highlights that fulfilling the accountability principle **does not necessarily mean that a controller is in compliance with the substantive principles** […], i.e., it does not offer a

> legal presumption of compliance nor does it replace any of those principles. […] In practice however, companies with a robust compliance program are according to the Working Party 29 more likely to be in compliance with the law." (*Sic*)

This position was reflected again in a subsequent Opinion[19] (Opinion 01/2012 on the data protection reform proposals adopted on March 23, 2012), which further confirms the accountability principle also applies in the context of data transfers, see p. 22:

> **"International transfers**
> The Regulation rightly emphasizes the accountability of data controllers to ensure that personal data remains protected when transferred outside of the European Economic Area (EEA). It facilitates data controllers by providing various "safe harbors" in the form of adequacy decisions, a streamlined system of BCRs for multinationals, approved contractual clauses and individual DPA approval. It also provides for various derogations in Article 44."

(c) EDPS Opinion on the revision of the Directive (January 14, 2011)

The EDPS supports the proposal of the WP29, and also supports an accountability principle applying to "all the elements of data protection law."[20] In its turn, the Commission in its EC Communication on revision of the Directive indicated that it "will explore ways of ensuring that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules. In doing so, it will take into account the current debate on the possible introduction of an "accountability" principle.[21]

(d) First EC proposal for a Regulation (December 25, 2012)

The EC's first proposal for a Regulation, basically implements the proposals of the WP29. According to the Explanatory Memorandum accompanying the EU Commission's first proposal[22] dated December 25, 2012, the provisions of Article 22 of the draft considered the debate on a "principle of accountability" and described in detail the obligation of responsibility of the controller to comply with the Regulation and to demonstrate compliance, by adopting internal policies and mechanisms for ensuring such compliance.

> **Article 5 sub (f):**
> "processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation
>
> **"Article 22**
> **Responsibility of the controller**
> The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with

[19] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf
[20] https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf
[21] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiDwYKqkdH5AhV-8rsIHd2uCawQFnoECAcQAQ&url=https%3A%2F%2Fwww.europarl.europa.eu%2Fdoceo%2Fdocument%2FLIBE-OJ-2011-06-15-1_EN.rtf&usg=AOvVaw2_FHIvg8EtiMdXz8NHZFl5
[22] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

this Regulation, including the assignment of responsibilities, and the training of staff involved in the processing operations."

Recital (60):
*"*Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation."

Note that Article 5(2) is based on Article 6(2) of the Directive, which embodied the original and narrower meaning of accountability *as responsibility for compliance*. The first draft of the EU Commission did not include a reference to the "accountability principle" and further did not include a reference to scalability (RBA) of the accountability provisions.

(e) First references to the RBA

Reference to a RBA can be found in the replies to a public consultation launched by the EU Commission, which clarified the rules for international data transfers, and in special adequacy decisions.[23] Comments from representatives of the academic community supported a more flexible approach and proposed the implementation of a RBA model which would be built on data controller's obligation to evaluate all relevant factors (e.g., the nature of the data, how long the data will be in the third country, whether the data will remain under the control of the data controller etc.). In this case, data transfer could take place even in situations where the general legal regime governing data protection was not similar to that as within the EU, but still reasonably effective in protecting individuals' core rights and interests.

(f) Note of the Presidency to EU Council on implementation of RBA (March 1, 2013)

Further to a first examination of the EU Commission proposal, the Presidency reported to the EU Council[24] that several Member States voiced their disagreement with the level of prescriptiveness of a number of obligations in the draft Regulation. At the same time, other Member States recalled the need to guarantee legal certainty in the Regulation. The Presidency of the EU Council (Cyprus) invited delegations to give their views on alternative ways of reducing administrative burden while maintaining the protection of individual rights. Many delegations stated that the risk inherent in certain data processing operations should be the main criterion for calibrating the data protection obligations. Where the data protection risk was higher, more detailed obligations would be justified and where it was comparably lower, the level of prescriptiveness should be reduced. The revised draft incorporated a 'horizontal clause' in Article 22 to incorporate the RBA.[25]

"**II. Risk-based approach.**

2. In the course of the first examination of the proposal for a General Data Protection Regulation, several Member States have voiced their disagreement with the level of

[23] See page 86 at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0072.
[24] https://data.consilium.europa.eu/doc/document/ST%206607%202013%20REV%201/EN/pdf.
[25] See para. 5 at https://data.consilium.europa.eu/doc/document/ST%206607%202013%20REV%201/EN/pdf.

prescriptiveness of a number of the proposed obligations in the draft Regulation. At the same time, some others have recalled the need to guarantee legal certainty in the proposed Regulation.

3. The Cyprus Presidency had already invited delegations to give their views on alternative ways of reducing administrative burden while maintaining the protection of individual rights. **Many delegations had stated that the risk inherent in certain data processing operations should be a main criterion for calibrating the data protection obligations. Where the data protection risk is higher, more detailed obligations would be justified and where it is comparably lower, the level of prescriptiveness can and should be reduced.**

4. At its December meeting, the Council instructed the DAPIX Working Party to continue to work on concrete proposals to implement a strengthened RBA in the text of the draft Regulation.

5. In accordance with this instruction the Presidency suggested amendments to the proposed Regulation as regards the text of Chapter IV (on the controllers' and processors' responsibility). **The revised draft of this Chapter includes a 'horizontal clause' in Article 22 of the Regulation, accompanied by a risk-based redrafting of many provisions of this Chapter (especially articles 23, 26, 28, 30, 31, 33, 34 and 35)."**

(g) EC Council Inter-institutional note amendments dated March 27, 2013

On March 27, 2013, the EU Council subsequently presented amendments to the draft, which changed the language of Article 22 to introduce the RBA:

> "Taking into account the nature, scope and purposes of the processing and the risks for the (...) rights and freedoms of data subjects, the controller shall implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation (…)."[26]

Recital 60 was amended as follows (bold and underlined in original text marking changes):

> **"The** responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged **to implement appropriate measures to ensure and be able** to demonstrate the compliance of each processing operation with this Regulation, **taking into account the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, such as excluding individuals from their rights or from the control over their personal data or giving rise to discrimination, identity theft or fraud, financial loss, damage of reputation or any other economic or social disadvantage. Where personal data are processed on behalf of the controller, the implementation of such measures should include in particular to use only a processor providing sufficient guarantees to implement appropriate technical and organizational measures. Where the processing is likely to represent specific risks for the rights and freedoms of data subjects, the controller or processor should carry out, prior to the processing an assessment of the impact of the envisaged processing operations on the protection of personal data. Guidance for the**

[26] See p. 23 at https://data.consilium.europa.eu/doc/document/ST-8004-2013-INIT/en/pdf

> **implementation of such measures by the controller could be given in particular by approved codes of conduct, approved certifications or guidelines of the European Data Protection Board, by a data protection officer, or, where a data protection impact assessment indicates that processing operations involve a high degree of specific risks, by the consultation of the supervisory authority prior to the processing. If proportionate, the verification of the obligations of the controller may be carried out by independent internal or external auditors or by providing an approved certification."**

Art. 5 sub (f) was changed into:

> "processed under the responsibility (…) of the controller (…)

Therefore basically reverting the language back to the text of its predecessor Article 6 (2) Directive. In the footnote accompanying this new provision (see nt 116) it was clarified that the accountability requirement was deleted in Article 5(f) as:

> "BE, LU, NO and FR thought turning the existing means obligation into a result obligation was too onerous and not realistic. As this also overlapped with Article 22 (1), the Presidency suggests deleting the latter part of this sentence here and set out the obligations on the controller in Article 22."

(h) WP29 Statement on the role of a RBA in data protection legal frameworks (May 30, 2014)[27]

In reaction to these developments in the EU legislative process, the WP29 issued a Statement on the role of a RBA in data protection legal frameworks, adopted on May 30, 2012. The WP29 clarifies in a number of crisp statements that the RBA should **not apply to the key rights granted to data subjects, which apply regardless of the level of risks incurred by the processing** and that controllers should always be accountable for compliance with the data processing obligations including by demonstrating compliance regarding any data processing, see p. 2.

> "However, the risk-based approach has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation. **It has been introduced recently as a core element of the accountability principle itself (Article 22)."**

From this Statement it can be derived that the WP29 was well aware that the changes proposed by the European Parliament and the Council constituted a major change as the RBA was now introduced as a core element of the accountability principle also impacting the underlying obligations of controllers rather than (just) the accountability measures themselves. The WP29 subsequently communicates the following key messages, stating that any scalability (RBA) should apply to the accountability measures only and not to the rights granted to data subjects, which should be protected regardless of the level of risk involved (bold added):

[27] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

1. Protection of personal data is a fundamental right according to Article 8 of the Charter of Fundamental Rights. Any processing operation, from collection to use and disclosure, should respect this key right.

2. Rights granted to the data subject by EU law should be respected **regardless of the level of the risks which the latter incur through the data processing involved** (e.g., right of access, rectification, erasure, objection, transparency, right to be forgotten, right to data portability).

3. There can be **different levels of accountability obligations** depending on the risk posed by the processing in question. However controllers should always be accountable for compliance with data protection obligations including **demonstrating compliance regarding any data processing whatever the nature, scope, context, purposes of the processing and the risks for data subjects are.**

(i) EU Council Interinstitutional File, Note on the RBA (July 3, 2014)

In this interinstitutional note on the RBA from the Presidency of the EU Council,[28] an overview is provided on the history and progress on the implementation of the RBA in the Regulation. Included are new proposals of the provisions where the RBA is further implemented (bold added).

"1. In the course of the first examination of the proposal for a General Data Protection Regulation, several Member States voiced their disagreement with the level of prescriptiveness of a number of the proposed obligations in the draft Regulation. At the same time, some others have recalled the need to guarantee legal certainty in the proposed Regulation.

2. Following an invitation by the Cyprus Presidency to give their views on alternative ways of reducing administrative burden while maintaining the protection of individual rights, **a common view emerged that the risk inherent in certain data processing operations should be a main criterion for calibrating the data protection obligations. Where the data protection risk is higher, more detailed obligations would be necessary and where it is comparably lower, the level of prescriptiveness can and should be reduced**.

3. At the JHA Council meeting in December 2012, DAPIX was instructed to work on concrete proposals **to implement a strengthened risk-based approach in the text of the draft Regulation**. During the Irish Presidency, very substantial steps were made towards incorporating such a risk-based approach in the text of the draft Regulation, in particular in Chapter IV (Controller and Processor), and in certain articles in Chapter III (Rights of the Data Subject).

4. As a consequence amendments were made to the proposed Regulation as regards the text of Chapter IV (on the controllers' and processors' responsibility). The revised draft of this Chapter **includes a 'horizontal clause' in Article 22 of the Regulation,** accompanied by a risk based redrafting of many provisions of this Chapter (especially Articles 23, 26, 28, 30, 31, 33, 34 and 35). Provisions with limited value-added (Articles 27 and 29) have been dropped. Equally, several important articles in Chapter III, including Articles 12, 14

[28] See p. 1 at https://data.consilium.europa.eu/doc/document/ST%2011481%202014%20INIT/EN/pdf.

and 15 were changed in order to ensure effective and efficient exercise of data subject rights, while improving certainty and transparency.

(…)

7. Whilst at the Council meeting on June 6-7, 2013, all delegations congratulated the Irish Presidency on the very important progress achieved in this regard, it is equally clear that many Member States are of the opinion that more efforts need to be undertaken to reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk based approach. Obviously this should be done whilst maintaining a high level of data protection.

8. To this end the Presidency is making a number if suggestions regarding further changes to Chapter IV and is inviting delegations to ask a number of questions.

9. Regarding the risk concept referred to in Article 22 and recitals 60, several delegations are of the opinion that this should be further detailed and that a description or definition of low risk should also be given. Delegations are invited to provide drafting regarding low risk situations.

(…)

15. The suggested clarification in Article 38(1)(f) is meant to enhance the risk-based approach by linking codes of conduct with the conditions for cross-border data flows to third countries, for the purpose of specifying the application of provisions of this Regulation. Article 33 has also been amended to state that compliance with codes of conduct should be taken into account for the purpose of a DPIA.

The new text for Article 22 was as follows:

Article 22

Obligations of the controller

1. Taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

(60) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should (…) be obliged to implement appropriate measures and be able to demonstrate the compliance of (…) processing activities with this Regulation (…). These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage;

- where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable individuals, in particular of children, are processed; or
- where processing involves a large amount of personal data and affects a large number of data subjects.

(j) Final text GDPR dated April 8, 2016

The final version of Article 24 came from the EU Council Position adopted on April 8, 2016.[29] In the draft statement[30] explaining its reasons, the EU Council stated it had strengthened the accountability of controllers and processors to promote a real data protection culture, and introduced **throughout the Regulation a risk-based approach, allowing for the modulation of the obligations imposed on controllers** (see p. 4) (bold added):

> "In order to achieve the objectives of the Regulation, the Council Position at first reading strengthens the accountability of controllers (responsible for determining the purposes and the means of the processing of personal data) and processors (responsible for processing personal data on behalf of the controller) so as to promote a real data protection culture. Against that background, **throughout the Regulation, a risk-based approach is introduced which allows for the modulation of the obligations of the controller and the processor according to the risk of the data processing they perform.** Furthermore, codes of conduct and certification mechanisms contribute to compliance with the data protection rules. This approach prevents overly prescriptive rules and reduces administrative burden without reducing compliance. Moreover, the dissuasive character of the potential penalties that can be imposed creates incentives for controllers to comply with the Regulation."

(k) Communication from the Commission on the EC Council position to the European Parliament (April 11, 2016)

In this communication,[31] the EC confirms that the position of the Council reflects the political agreement reached between the European Parliament and the Council in informal trilogues on

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016AG0006%2801%29.
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_ADD_1&from=EN.
[31] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52016PC0214.

December 15, 2015, subsequently endorsed by the Council on April 8, 2016. The Commission supports this agreement since it is in keeping with the objectives of the Commission proposal:

> "The agreement also preserves and further develops the risk-based approach already present in the Commission proposal and which requires that controllers and, in some cases the processors, to take into account the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of the data subject of such processing."

7.3. Conclusions based on the legislative history of the GDPR

Inclusion of Article 5(2) seems to be based on Article 6(2) of the Directive ("It shall be for the controller to ensure that paragraph 1 is complied with"), which embodied the original and more narrow meaning of accountability as responsibility for compliance. It was at the proposal of the European Parliament to maintain the original proposal of the EC and bring this provision more into line with accountability ('be able to demonstrate' rather than 'demonstrate') and the addition of the word 'accountability' in brackets at the end.[32] The Council proposed instead to concentrate on responsibility.[33] The resulting compromise was a combination in Article 5(2) of responsibility proposed by the Council and demonstrability and the label 'accountability' in brackets proposed by the Parliament.[34] There are no indications in the legislative history why the accountability element in Article 5(2) was first included, then deleted and then reinstated, but without the RBA. As this provision must have meaning (why otherwise reinstate it), it seems justified to conclude that the RBA does not apply to the material processing principles of Article 5.

The actual principle of accountability as inspired by the proposals of the WP29 found its way into Article 22 (now 24). It is unclear why the EC declined to use the term accountability principle in the text or heading of Article 22 itself. It is only in the Explanatory Memorandum (at para. 3.4.4) that it is explained that Article 22 [now 24] "takes account of the debate on a 'principle of accountability'". The heading further referred to "responsibility of the controller," which fitted more the compliance notion of Article 5(2). It is clear that the EC in its first draft proposal for the Regulation, included the accountability principle as advocated by the WP29, whereby the provision applied to the standard of evidence only and not also to the underlying obligations of the controller, and where the RBA applied to the scalability of the standard of evidence only. Based on the legislative history it is however undisputable that subsequent changes to the initial Article 22 were introduced by the Council in order to incorporate a horizontal provision applying the RBA for all obligations of the controller, and specifically also for the data transfer obligations.

An analysis of the legislative history, therefore confirms the assessment based on a textual analysis of the GDPR (see for conclusions sub 6.1 above).

8. Assessment of Schrems II

[32] See Amendment 99, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=EN.
[33] See p. 83 at https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.
[34] Cf. supra n. 3, p. 113.

Reviewing the ECJ judgement in Schrems II,[35] the Austrian DPA is correct that the ECJ does not refer to the accountability principle or the RBA under the GDPR. The conclusion of the Austrian DPA, however, that the ECJ (therefore thus) does not take a RBA to data transfers cannot be based on this judgement. What the ECJ did in the Schrems II was raising the bar for international data transfers based on Article 46 (transfers based on appropriate safeguards) to the so-called **essentially equivalent level,** this in reference to the general principle for transfers of Article 44 and the EU Charter of fundamental rights. In the absence of an adequacy decision, the ECJ considers it the **responsibility of the controller** to make a transfer assessment before a transfer can take place on the basis of appropriate safeguards, which also includes an assessment of the laws **and practices** of the country or countries where the data are flowing to (see para. 126: where the ECJ explicitly refers to "the law and practices in force in the third country concerned" and requires "(...) ensuring, **in practice**, **the effective protection** of personal data transferred to the third country concerned."[36] The controller should then take measures to compensate for any lack of data protection by way of appropriate safeguards. It is important to note that the Court does not require that additional safeguards provide a 100% guarantee that access to data by third parties can never occur, but rather that they constitute "effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law…" (para. 137). Though the ECJ did not explicitly refer to the accountability principle of Article 24, this transfer assessment obligation of the controller seems in line with the RBA of the accountability principle of Article 24.

See below para. 131 – 134 of Schrems II (bold added)

> "131. In that regard, it must be borne in mind that, according to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject' and that 'those safeguards **should ensure compliance with data protection requirements** and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies … in the Union or in a third country'.
>
> 132. Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, as is clear from paragraph 125 above, but that **Article 44**, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of **Articles 7, 8 and 47 of the Charter**, require that the level of protection of natural persons guaranteed by that regulation is not undermined, **it may prove necessary to supplement the guarantees contained in those standard data protection clauses**. In that regard, recital 109 of the regulation states that 'the possibility for the controller … to use standard data-protection clauses adopted by the Commission … should [not] prevent [it] … from adding other clauses or additional safeguards' and states, in particular, that the controller

[35] Cf. supra n.4.
[36] ibid. see para. 126.

'should be encouraged to provide additional safeguards … that supplement standard [data] protection clauses.'

133. It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

134. In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."

This is also confirmed by the dictum of Schrems II. The dictum provides that the *relevant aspects of the **legal system** of the third country* need to be taken into consideration, therefore not only the law of the relevant third country, but also its practices, as also follows from para. 126 of Schrems II. The ECJ refers for relevant aspects to the not-limitative list of elements in Article 45(2) GDPR, which the EC needs to consider when performing an adequacy assessment of a third country. The list of Article 45(2) shows that the EC in its assessment not only needs to assess the law of the country, but also "*the effective functioning*" of the law. In other words, all relevant aspects of the legal system in practice. See the dictum:

> "To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the **relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation**."[37]

9. Assessment EDPB Recommendation

The EDPB in the Recommendation[38] reflects the Schrems II judgement in a similar manner. The EDPB indicates that the Schrems II judgement "reminds us that the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes," that "the Court also asserts this by clarifying that the level of protection in third countries

[38] Cf. supra n.5.

does not need to be identical to that guaranteed within the EEA but **essentially equivalent**," that the "Court also upholds the validity of standard contractual clauses, as a transfer tool that may serve to ensure contractually an essentially equivalent level of protection for data transferred to third countries," but that these "do not operate in a vacuum" and that:

> "controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In those cases, the Court still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. The Court does not specify which measures these could be. However, the Court underlines that exporters will need to identify them on a case-by-case basis. **This is in line with the principle of accountability of Article 5.2 GDPR, which requires controllers to be responsible for, and be able to demonstrate compliance with the GDPR principles relating to processing of personal data.**

It is noteworthy that the EDPB explicitly refers to the accountability principle of Article 5(2), but does not in any way refer to the accountability principle of Article 24. The EDPB in para. 1 of the Recommendations explicitly considers that the accountability principle of Article 5(2) GDPR[39] also applies to data transfers "since they are a form of data processing in themselves."[40] I recall (see sub 7.1 above) that the Article 5(1) lists the general processing principles, but that these do not include the data transfer principles. The EDPB is correct in considering a transfer a processing, but this then entails that the material principles apply to transfers, but this cannot carry the conclusion that transfers are thus a material principle in themselves. This goes against the system of the GDPR where the transfer rules have their own Chapter V. The underlying reason for the EDPB to find this 'work around' is that the accountability principle of Article 5(2) – as I also concluded - does not have the RBA as to compliance of the material principles, where the accountability principle of Article 24 does have the RBA for compliance of the obligations of controllers. By taking this position, the EDPB basically pushes its own version of the accountability principle as proposed by the WP29 at the time for revision of the Directive, which was, however, ultimately not adopted by the EU regulator. Noteworthy is, however, that despite the reference to Article 5(2) GDPR, the final version of the Recommendation does include language (however nominally) to allow for a RBA of data transfer assessments, though the threshold seems high. A more kind interpretation is that the EDPB is confused by the fact that Article 5(2) does include the reference to "accountability," while Article 24 does not (see sub 4 above). I, however, do not believe the EDPB is confused here, but actually pushes its version of accountability principle as it advocated from the start, while normally covering its basis by including a nominal RBA into the Recommendations itself in line with Schrems II. That the RBA is indeed (though

[39] See para. 3 where the EDPB refers to the accountability principle and includes in footnote 12 again a reference to Article 5(2) GDPR only. See also para. 5, footnote 18; para. 48, footnote 58; and para. 76, footnote 77. The only reference to Article 24 can be found in footnote 22, which seems an oversight more than intentional.

[40] The EDPB refers to para. 45 of Schrems II. However, in this paragraph the ECJ just indicates that a transfer is a processing (which is correct), but this is not in any way related to how Article 5(1) GDPR should be interpreted.

somewhat nominally) included in the Recommendations can be derived from the changes made by the EDPB in the initial version after consultation.

The initial consultation version of the Recommendations,[41] did not take a RBA as to the transfer assessment. The consultation version even specifically indicated that organizations should "not rely on subjective [factors] such as the likelihood of public authorities' access to your data in a manner not in line with EU standards' (see para 42). Following the consultation phase, whereby many stakeholders provided as input that the EDPB had wrongfully ignored the RBA of the GDPR, the above statement was no longer included in final version. Instead, the EDPB (somewhat nominally, and without any explicit acknowledgement) included the RBA approach, though the threshold to do so is very high. This is reflected in the text by including in a number of places that the transfer assessment should not only include the laws, but also the **practices** in the relevant third country (which was also specifically referred to by the ECJ in the Schrems II judgement, see sub 8 above),[42] but most importantly by allowing controllers to proceed with the transfer without supplementary measures if they consider the likelihood of a negative impact of the legislation or practices in a third-country negligible.

See Section 1 on the accountability of data transfers (bold added):

> "1. ACCOUNTABILITY IN DATA TRANSFERS
>
> 1. EU primary law considers the right to data protection as a fundamental right. Accordingly, the right to data protection is afforded a high level of protection and limitations may only be made if they are provided for by law, respect the essence of its right, are proportionate, necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.
>
> 2. An essentially equivalent level of protection to that guaranteed within the EU must accompany the data when it travels to third countries outside the EEA to ensure that the level of protection guaranteed by the GDPR is not undermined, both during and after the transfer.
>
> 3. The right to data protection has an active nature. It requires exporters and importers (whether they are controllers and/or processors) to go beyond an acknowledgement or passive compliance with this right. Controllers and processors must seek to comply with the right to data protection in an active and continuous manner by implementing legal, technical and organizational measures that ensure its effectiveness. Controllers and processors must also be able to demonstrate these efforts to data subjects and data protection supervisory authorities. This is the so called principle of accountability.
>
> 4. The principle of accountability, which is necessary to ensure the effective application of the level of protection conferred by the GDPR **also applies to data transfers to third countries since they are a form of data processing in themselves**. As the Court

[41] Cf. supra n.5.
[42] Cf. supra n.4.

underlined in its judgment, a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR read in the light of the Charter must be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.

5. In the Schrems II judgment, the Court emphasizes the responsibilities of exporters and importers to ensure that the processing of personal data has been and will continue to be carried out in compliance with the level of protection set by EU data protection law and to suspend the transfer and/or terminate the contract where the importer of the data is not, or is no longer, able to comply with standard data protection clauses incorporated in the relevant contract between the exporter and the importer. The controller or processor acting as exporter must ensure that the importers collaborate with the exporter, where appropriate, in its performance of these responsibilities, by keeping it informed, for instance, of any development affecting the level of protection of the personal data received in the importer's country. These responsibilities are an application of the GDPR principle of accountability to the data transfers."

See for the inclusion of the RBA para 43 of the Recommendations:

43. Your assessment must be based first and foremost on legislation publicly available. **Examining also the practices of the third country's public authorities will allow you to verify if the safeguards contained in the Article 46 GDPR transfer tool can be a sufficient means of ensuring, in practice, the effective protection of the personal data transferred.** Examining the practices in force in the third country will be especially important for your assessment in the situations described below.

And in particular para. 43.3:

"43.3 The assessment may reveal that relevant legislation in the third country may be problematic and that the transferred data and/or the importer at hand fall or might fall within the scope of this problematic legislation. In light of uncertainties surrounding the potential application of problematic legislation to your transfer, you may then decide to:

- Suspend the transfer;

- Implement supplementary measures to prevent the risk of potential application to your importer and/or to your transferred data of laws and/or practices of the third country of the data importer, which are capable of impinging on the transfer tool's contractual guarantees of an essentially equivalent level of protection to that guaranteed in the EEA; or

- Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, **if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer.** You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below. Therefore, you will need

to have demonstrated and documented with a detailed report that problematic legislation will not be applied in practice to your transferred data and/or importer, and, consequently, that it will not prevent the importer from fulfilling its obligations under the Article 46 GDPR transfer tool."

10. Overall conclusions

Based on an analysis of the text of the GDPR, the legislative history, the Schrems II judgement and the EDPB Recommendations the conclusions as to the interpretation of the GDPR are:

- The accountability requirement of Article 24 incorporates the RBA. Article 24 has a horizontal application and the RBA therefore applies not only to the standard of evidence (accountability measures required), but also to the underlying obligations of the controller in the GDPR. Where the transfer rules are stated as obligations of the controller (rather than as absolute principles), the RBA of Article 24 therefore applies.

- The accountability principle of Article 24 does not apply to the general processing principles of Article 5(1). The accountability principle of Article 5(2) applies to the general processing principles, which do not include the data transfer principles. Article 5(2) does **not** include the RBA.

- The ECJ in Schrems II has raised the bar as to data transfers based on Article 46 (transfers subject to appropriate safeguards), in the sense that when personal data are transferred these require an **essentially equivalent** level of protection (rather than an adequate level), this in reference to the general principle for transfers of Article 44 and the EU Charter of fundamental rights. In the absence of an adequacy decision, the ECJ considers it the **responsibility of the controller** to make a transfer assessment before a transfer can take place on the basis of appropriate safeguards, which also includes an assessment of the laws **and practices** of the country or countries where the data are flowing to in order to ensure **in practice**, **the effective protection** of personal data transferred to the third country concerned." The controller should then take measures to compensate for any lack of data protection by way of appropriate safeguards. The ECJ does not require that additional safeguards provide a 100% guarantee that access to data by third parties can never occur, but rather that they constitute "effective mechanisms that make it possible, **in practice**, to ensure compliance with the level of protection required by EU law…." Though the ECJ did not explicitly refer to the accountability principle of Article 24, this transfer assessment obligation of the controller seems in line with the RBA of the accountability principle of Article 24.

- The EDPB Recommendations confirm that Schrems II is in line with the accountability principle and that this principle applies also to the data transfer rules. Though the EDPB Recommendations refer to the accountability principle of Article 5(2) GDPR only, the EDPB Recommendations seems to allow for a nominal RBA as to the transfer assessment, this in line with the RBA of Article 24 GDPR and Schrems II.

- The EDPB is mistaken where it applies the accountability requirement of Article 5(2) also to the transfer requirements. The underlying reason for the EDPB to apply

Article 5(2) rather than the accountability principle of Article 24, is likely that the accountability principle of Article 5(2) does not have the RBA as to compliance of the material principles, where the accountability principle of Article 24 does have the RBA for compliance of the obligations of controllers. By taking this position, the EDPB basically pushes its own version of the accountability principle as proposed at the time for revision of the Directive, which was, however, ultimately not adopted by EU regulators.

***

BIBLIOGRAPHY

Article 29 Data Protection Working Party, "Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks," 14/EN, WP218 (2014) at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Article 29 Data Protection Working Party, 'Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)' (1998), at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (2010) at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

Article 29 Data Protection Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (2009) at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

Paul Breitbarth, "A Risk-Based Approach to International Data Transfers," EDPL, 2021, pp. 539 – 549 at https://edpl.lexxion.eu/data/article/17963/pdf/edpl_2021_04-010.pdf

Centre for Information Policy Leadership, "A Risk-Based Approach to Privacy: Improving Effectiveness in Practice," 2014 at A Risk-based Approach to Privacy: Improving Effectiveness in Practice (informationpolicycentre.com)

CNIL, at Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply | CNIL

CNIL, at Questions and answers on the CNIL's formal notices concerning the use of Google Analytics | CNIL

EDPB, at Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)

FATF, "Guidance for a Risk-Based Approach for Legal Professionals," FATF, Paris, at www.fatf-gafi.org/publications/documents/Guidance-RBA-legal-professionals.html

Information Accountability Foundation, There are Many Reasons to Worry About Data Transfers, but the Austrian DPA Second Google Analytics Decision Should not be one of Them, May 4, 2022, at There are Many Reasons to Worry About Data Transfers, but the Austrian DPA Second Google Analytics Decision Should not be one of Them - The Information Accountability Foundation

Gellert Raphaël, "We Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection," EDPL, 2016 at We have always managed risks in data protection law: Understanding

the similarities and differences between the rights-based and the risk-based approaches to data protection — Tilburg University Research Portal

Gellert Raphaël, "The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission Proposed Artificial Intelligence Act: business as usual?" Journal of Ethics and Legal Technologies, Volume 3(2), November 2021 at The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act. Business as usual ? (ru.nl)

Gellert Raphaël, *The Risk-Based Approach to Data Protection,* Oxford Data Protection and Privacy Law, p. 277.

Gonçalves Maria Eduarda, "The Risk-Based Approach under the New EU Data Protection," *Journal of Risk Research,* 2019 12 vol. 23 iss. 2 at https://www.tandfonline.com/doi/full/10.1080/13669877.2018.1517381

Kuner Christopher, 'Schrems II Re-Examined' (VerfBlog, August 25, 2020), at https://verfassungsblog.de/schrems-ii-re-examined/

Kuner Christopher, Bygrave Lee and Docksey Christopher, *The EU General Data Protection Regulation: A Commentary. Update of Selected Articles.* Oxford University Press, 2021 at The EU General Data Protection Regulation: A Commentary/Update of Selected Articles by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler, Luca Tosoni :: SSRN

Maldoff Gabriel, "The Risk-Based Approach in the GDPR: Interpretation and Implications," IAPP at White Paper – The Risk-Based Approach in the GDPR: Interpretation and Implications (iapp.org)

NOYB, "Austrian DPA rejects 'risk based approach' for data transfers to third countries." at UPDATE on noyb's 101 complaints: Austrian DPA rejects "risk based approach" for data transfers to third countries

Quelle Claudia, "Enhancing compliance under the general data protection regulation: the risky upshot of the accountability- and risk-based approach," European Journal of Risk Regulation, 9, 2018, pp. 502-526 at Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach | European Journal of Risk Regulation | Cambridge Core

Viterbo Francesco Gacomo, "The User-Centric and Tailor-Made-Approach of the GDPR through the Principle sit Lays Down," Italian Law Journal, 631, 2019 at (PDF) The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down | Francesco Giacomo Viterbo - Academia.edu