July 2026

Unravelling the GDPR costs enigma for future action: a Better Regulation perspective

By Henk (H.M.) Griffioen, Dutch Advisory Board on Regulatory Burden (ATR), on behalf of RegWatchEurope[1]

Practical experiences with the application of the EU General Data Protection Regulation (GDPR) have been at the forefront of public attention since its entry into force. Its implementation in company practices was a major operation at the time. To the current day, indications are that many (especially smaller) companies struggle to grasp what exactly is expected of them. Even public authorities can tend to err on the side of caution by making the GDPR more intimidating than it was ever intended to be.[2]

Such substantive stumbling blocks are well documented and addressed by reports, consultations, evaluations and most recently Omnibus Packages of the European Commission. Surprisingly though, the directly connected question of what we as societies are paying for our data protection does not enjoy the same prominence or serious consideration, as quantitative analysis turns out to be sparse and confusing.

This essay traces back the evidentiary trail of cost calculations all the way back to the original Impact Assessment of the GDPR in 2012, including the reception by Member States. We find that this trail is hard to make sense of. It is not possible to state the costs of the GDPR with any semblance of confidence, or to come across an overarching analysis of all the impacts of the obligations that it imposes. This is all the more remarkable since cost calculations are in theory one of the cornerstones of the Better Regulation regime that spans the EU and its Member States.

In this essay, a number of ways are addressed to strengthen the conversation about costs of European legislation. In so doing, we are not passing judgement on the merits of the GDPR, or on the proper 'price' that we should be willing to pay for the protection that it provides and for its unlocking of the economic opportunities of safe data traffic. Our core concern is with the transparency of costs as a prerequisite for sound political decision-making. The lack thereof casts a particular light on the ongoing negotiations (at the time of writing) on the Digital Omnibus package.

The General Data Protection Regulation

The General Data Protection Regulation (GDPR; EU 2016/679) is undoubtedly one of the most important and well-known pieces of EU legislation. While its inception dates back around 15 years,[3] it has been fully applicable since 2018, and has already completed two rotations of the policy cycle, in that the second evaluation has been published in 2024.[4] At face value, all the trusted elements of the European Better

[1] I am grateful to those within RegWatchEurope and outside of it (academic, civil service, advocacy) who made valuable comments on draft versions of this essay.
[2] See e.g. Algemene Rekenkamer (Dutch Court of Auditors), *Omgang met de AVG in relatie tot uitvoering overheidstaken*, March 2023; https://www.rekenkamer.nl/documenten/2023/03/30/omgang-met-de-avg-in-relatie-tot-uitvoering-overheidstaken.
[3] The EU impact assessment is from 2012; SEC (2012) 72.
[4] COM (2024) 357; see also COM (2020) 264 and SWD (2020) 115.

Regulation regime are there: an EU Impact Assessment (hereafter IA or EU IA[5]), a RSB (then called IAB) scrutiny report,[6] national follow-up exercises, evaluations, and very recently proposed revisions by means of the fourth and seventh Omnibus packages.[7]

As one may have noticed from this introduction, we are looking at the GDPR from a very specific perspective. As RegWatchEurope, being a network of regulatory scrutiny bodies, we can provide viewpoints on the quality of the policy cycle in terms of the evidentiary basis, but we cannot pretend any authority as to the substance of the Regulation. This essay is therefore not about the merits or success of the GDPR as such, but rather about the question whether the evidentiary basis for political decision making was – and is – fit for purpose.

In the case of the GDPR, it should be stated at the outset that a substantial rise in the regulatory costs surrounding processing of personal data was entirely foreseeable. The previous Directive 95/46 was enacted at a time (1995) when internet commerce and personal data as a business model were a fraction of what they now are. The information society runs on data, and if we want some security, protection and due process along the way, we will need to pay for it.

But how much are we paying for data protection? And who picks up the bill? This is the actual subject of this essay, and it presents a puzzling picture. Recognizing that the GDPR contains both benefits and costs to administrations, businesses and citizens, our argumentation is mainly limited to the costs to business.

Cost assessment: cornerstone or afterthought?

The ex ante approximation of regulatory burden8 is an entirely uncontroversial element of the Better Regulation regime that the EU and Member States share. One could call it the most basic of all requirements, because it doesn't presuppose complex and state of the art methodologies, but 'simply' an informed and sane application of the Standard Cost Model (SCM), which has become universal for this purpose in Europe.9 That is not to say that this exercise is always easy, because it does remain an ex ante prognosis, with all the uncertainties that this entails. Especially with a vast and complex Act like the GDPR, which permeates all strata of societal life, the assessment of costs requires a major effort. It is virtually impossible to hit the nail squarely on the head in every respect, which is why it is also important to revisit the cost assessment once the facts on the ground are starting to become clearer. In our Position Paper on interim evaluations, which took its lead from the vicissitudes of the Corporate Sustainability Reporting Directive, RegWatchEurope argued for a more systematic way of keeping cost assessments up to date, also after a European Act has entered into force.[10] Generally speaking, the cost dimension of an Act is at risk of falling off the table in the course of the policy cycle. So there are still things to be wished for. As we will see, the GDPR file is a prime example of this.

[5] Although strictly speaking such IAs don't stand for the findings of the EU as a whole but only of the European Commission, we will continue to refer to them as EU IAs because they serve as a reference point throughout the EU and also in Member States.
[6] This Report has, as far as we can reconstruct, not been published.
[7] Underlying report on small midcap companies: SWD (2025) 501. Digital Omnibus: COM (2025) 836 and SWD (2025) 836.
[8] Comprising of the cost of abiding by information requirements and substantive requirements.
[9] We are taking the SCM model to apply to both the calculation of administrative burdens and substantive compliance costs (sometimes called adjustment costs), even though the Commission Better Regulation Toolbox states that the latter is not strictly the case. To our minds however, the parallels between these types of calculations are more important than the differences, and the calculation of substantive compliance costs would benefit from clearer guidance.
[10] https://www.regwatcheurope.eu/wp-content/uploads/2025/04/RWE-Position-Paper-The-case-for-lean-interim-evaluation-as-a-means-towards-adaptive-EU-assessment-cycles-final.pdf

The problem is however not only about the closing of the policy cycle. Already at the outset, EU IAs do not always treat cost calculations as the cornerstone. One very important circumstance, which also causes problems in the 'translatability' to the national context, is that IAs usually only summarise the cost calculations under very broad headings, instead of showing the full picture along the lines of all the legal obligations that an Act entails. In other words, one is told that the SCM has been applied, but this is not shown – and therefore not replicable with national data. The adage 'show, don't tell' would make the conversations about regulatory burdens between European Institutions and Member States a whole lot easier. RegWatchEurope has recently addressed this problem in more detail in an Opinion on the 'granularity' of published cost calculations.[11]

Within RegWatchEurope, all members are involved in assessing the effects of EU legislation, be it directly though scrutiny of EU proposals, or indirectly through scrutiny of national implementation, or both. RegWatchEurope members can arrange or press for national follow-up exercises, if they assess that the cost impacts for their jurisdictions are unclear. These follow-up exercises could potentially enrich and correct the picture that a EU IA has painted. However, the conversation as to how an IA relates to findings in the Member States is hard to start up. In practice an EU IA will simply stand side by side with a national follow-up assessment, despite possibly wide disparities in findings.

Before we take a deeper dive into the cost calculations of the GDPR file, a remark is in order on why it is important to have a good overview[12] of the regulatory burden even now, years after its entry into force. The GDPR is hardly going to be repealed because of this factor. The answer is that regulatory burden is not just a number but represents the actual effort that companies and citizens must make. An authoritative assessment of that effort helps a great deal in the discussions on competitiveness and practicability. Remarkably, even though the cost dimension of the GDPR is and in a sense has always been rather enigmatic, the discussion of its competitiveness effects and practical implementation problems has been very lively. So contrary to the conversation about costs, the conversation about practical implications and bottlenecks has been lively, even if missing an important piece of information at its core.

Cost-conversation stoppers in the GDPR file

We would like to stick by the metaphor of conversation. In our context, a successful conversation about costs is one in which the different partners understand each other, share assumptions, process and further each other's findings, and reach an authoritative conclusion or a common understanding. In the following, the GDPR file will be analysed by way of a number of conversation stoppers that have hindered this outcome. They vary from structural concerns to more GDPR-specific circumstances.

The cost-conversation has prematurely stopped with regard to the GDPR. Neither of the EU-level Evaluation Reports (2020 and 2024) [13] contains any mention of regulatory burden. Nor, as far as we can see, has any Member State pressed for a reassessment of GDPR regulatory burden, or revisited it in national evaluations. Regulatory burdens have made a reappearance in the proposed revision of the GDPR by means of the fourth Omnibus package by which the newly to be defined category of midcap companies would receive an exemption from the obligation to document personal data processing (about which more below). But the savings calculated at that occasion bear no relation to earlier assessments, and they treat the cost dimension

[11] https://www.regwatcheurope.eu/wp-content/uploads/2025/12/RWE-Opinion-on-Granularity-of-EU-Cost-Calculations.pdf

[12] Cost calculations concerning particular obligations can of course also serve as inspiration for targeted amendments. In other words, cost calculations are not an all-or-nothing affair, but fulfil many functions in policy development, deliberation and upkeep. As they stand, EU IAs generally do not provide the groundwork for such targeted insights.

[13] Above, fn. 4.

of the GDPR as a blank slate. Perhaps even more importantly than the fourth Omnibus, the seventh edition (Digital/AI Omnibus) tackles and corrects several key stumbling blocks in the application of the GDPR that stakeholders had put before the Commission. In the Staff Working Document that stands in for a full IA,[14] it is stated that for none of these proposed changes calculations of costs could be made.[15] Without going into the details of the proposal, we can state that this impossibility is far from self-evident, seen through the lens of regulatory scrutiny bodies. Regardless, even if the Digital Omnibus had calculated the savings vis-à-vis the current situation, the enigma of what that current situation entails – i.e. what the base line cost of the GDPR is – would remain the same.

Going further back in time, has the conversation about the costs incurred through the GDPR ever properly started? The original IA stated that the GDPR would bring about a net total of €2,3 billion in burden reduction. This was mainly due to a decrease in legal fragmentation which drives up costs for doing business across European borders. At face value – but we will go into this in greater detail - the GDPR provides a far more integrated regime than the preceding Directive 95/46. The original IA interpreted the shift to a Regulation instead of a Directive as a prompt to conclude that companies would no longer need to familiarise themselves with different rulebooks. Of the whole IA, this dimension is the most fully analysed, leading to €2.9 billion stated burden reduction. In terms of new sources of costs, the IA reports on three categories under very broad headings, which are difficult to even match with identifiable clusters of GDPR obligations. In total, the GDPR would only add about €778 million in new cost categories to the existing Directive, hence the conclusion that the GDPR as a whole would cause a substantial net saving. In hindsight, these numbers do not appear in the least realistic. And there is another problem. As was customary at the time, the IA does not contain a full assessment of substantive compliance costs. The one element the IA does elaborate on is the average cost of a single Data Protection Impact Assessment, one of the new requirements of the GDPR. For reference on the importance of substantive compliance costs: a Dutch report from 2013 assessed the costs of one single GDPR requirement to be €500 million (at the upper range) in the Netherlands alone.

Having covered the headlines of the IA from 2012 and the ensuing policy cycle(s), we can proceed to the factors which have further impeded the development of a veritable cost conversation. From these seven so-called conversation stoppers, lessons can be gleaned which can be brought to bear on the Better Regulation system in general, but also on a specific trajectory like the Digital/AI Omnibus.

Conversation stopper I: sparse, stand-alone national follow-up assessments

For this essay, we analysed all the on-the-record national follow-up to the Better Regulation aspects of the GDPR in Finland, Germany, Sweden, the Netherlands, Norway and Denmark. Of these countries, Sweden (2019)[16] and the Netherlands (2013)[17] stand out as there has been a real, robust quantitative assessment of regulatory burdens done there.[18] Of the two, the Dutch assessment could have had an impact on the negotiations of the GDPR as they were still ongoing at the time, while the Swedish assessment was done in the implementation phase. The responsible Dutch Minister expressed concern about the findings – between

[14] See our Opinion on the Omnibus process: https://www.regwatcheurope.eu/wp-content/uploads/2026/05/RWE-omnibus-project-results-and-recommendations-FINAL-3.pdf.
[15] I.e. with regard to core requirements of the GDPR. There was a calculation of savings due to a simplification of data breach reporting requirements, but these are not attributable to the GDPR because they are caused by overlaps with subsequent legislation (e.g. the Digital Operational Resilience Act). The main thrust of the savings presented by the Commission is provided by the simplification of cooky-related requirements, but they also do not stem from the (original scope of the) GDPR.
[16] Unpublished ex ante calculations, summarized in "Annual report on regulatory costs 2018" (The Swedish Agency for Economic and Regional Growth, 2019, Dnr Ä 2015-274).
[17] https://www.eerstekamer.nl/eu/publicatie/20130621/toetsing_europese/document
[18] A vast proportion of the materials studied did not contain cost calculations and will not be referenced in this essay.

€1,1 and 1,4 billion in estimated compliance costs in the Netherlands alone as compared to €70 million under the previous Directive – and announced that he would bring these figures to the European negotiating table.[19] But it is unknown and rather hard to trace what the effect of this Brussels confrontation was. Something similar applies to the Swedish case. In 2013, the Swedish Better Regulation Council stated that there were missing cost analyses in the EU IA for several proposed requirements, and called for a national complementary IA (which in the end was only conducted much later).[20] To get an idea of the magnitude of the findings in the Dutch and Swedish contexts, we can zoom in on the obligation that is also the subject of the fourth Omnibus revision, namely the obligation to keep records and documentation of all personal data processing ready for a possible request by the Data Protection Authority (DPA). This obligation was estimated to cost Swedish business €975 million one-off and €110 million yearly[21] (neither corrected for inflation since 2019). The findings for Dutch business were in a range between €156 million and the aforementioned €500 million (not corrected for inflation since 2013), however not making a distinction between one-off and recurring costs. The record in Germany, Finland, Denmark and Norway shows varying degrees of quantification but of a more fragmented sort, and furthermore a lot of discussion on the substance of practical implementation problems.

What stands out from this is of course the wide gap between the EU assessment and the national ones, with the latter concluding that the GDPR would be far more costly than the official record shows. But there are also institutional observations to be made. It is clear from this case file but also from the broader experience of RegWatchEurope that the occurrence of national follow-up exercises is very uneven. For an Act such as the GDPR, where to call it important and impactful qualifies as an understatement, it is surprising to see such sparsity of analysis. Also on the institutional plane, we can observe that the follow-up efforts that were performed bear no analytical relation to the EU IA and never incited a reaction from the Commission. These exercises were done as if the GDPR file was a blank slate, and in no way make use of the EU IA provided. In short, these exercises redo the assessment instead of revisiting it on the national level. The EU, Dutch and Swedish exercises also cluster the obligations in different ways, which makes them hard to compare to each other as well.

Conversation stopper II: lack of granularity of the EU IA

For a proper validation and to be able to extrapolate findings to the national contexts, a certain degree of granularity of calculations is indispensable. What is usually provided in an EU IA is an overview of the conclusions as to regulatory burdens on the meso level, for instance clustered by groups of obligations, thus leaving the calculations on individual legal obligations unpublished. What is then also mostly[22] missing is the groundwork of the SCM: how many companies are covered, how many hours they will have to spend on the obligations, or how much they will spend out-of-pocket in case of outsourcing. This makes it very difficult to replicate or verify the assessment by performing an integrated follow-up assessment. There appears to be a lot of untapped potential here, as the EU possesses an overarching statistical system which can provide e.g. company codes that would make the estimation of national impacts far easier. The groundwork of the SCM is undoubtedly done behind the scenes, but as mentioned above it would be helpful to 'show, don't tell' on the public record what the expected burdens will be. As we already mentioned in our Opinion on this 'granularity' issue, the importance and frequency of national follow-up assessments is very likely to grow

[19] Tweede Kamer (Dutch House of Representatives), 32761, nr. 50.
[20] Statement on the European Commission impact assessment, the Swedish Better Regulation Council, (N 2008:05/2012/529), unpublished.
[21] Note that these estimates were not compared to the estimated costs of the previous existing data protection legislation. This is not a current practice, but was exceptionally made for the GDPR for cost and time reasons.
[22] The GDPR IA does provide a rudimentary indication of (inter alia) the hours spent per company because of the aforementioned legal fragmentation.

further. In the current circumstances, it is practically difficult to tie these assessments in with the EU IA. Integration of Better Regulation efforts between the EU and Member States really starts with the necessity of having real (published) SCM calculations at one's disposal.

Conversation stopper III: estimating compliance costs

We already mentioned the fact that the EU IA on the GDPR hardly contained any information about substantive compliance costs. Notwithstanding the uncertainties of the file, it appears safe to say that these costs are some orders of magnitude larger than the administrative costs that the IA did assess. In hindsight, the IA shouldn't have congratulated itself on a burden reduction of €2,3 billion, regardless of the question if this conclusion was adequate as a matter of administrative costs only. In the aftermath of an IA, such conclusions can start to lead a life of their own and it has indeed been echoed many times that the GDPR would lead to a reduction in regulatory burden, which was never realistic and certainly hasn't become more realistic over time.

Over time, it has become common that EU IAs do cover substantive compliance costs as well. That is a good development, but we would like to point out some remaining problems. First and most obviously, this assessment of substantive compliance costs was never done retrospectively for the GDPR at the EU level, which still leaves us without an authoritative overview of what we are paying for our data protection. Secondly and more generally, even if the inclusion of substantive compliance cost calculations is undoubtedly an improvement, its execution typically makes blind spots manifest in EU IAs. It is often the case that a certain heading (cluster of obligations) contains the announcement that there was not enough data and that no conclusion could be reached. The Digital Omnibus is a case in point – notwithstanding that it reports savings rather than additional costs – as it states that none of the core amendments proposed to the GDPR could be quantified. Unfortunately, in the further process – also of negotiations – this 'unknown burden' is for all intents and purposes translated as 'zero burden' even though these omissions tend to concern very important categories of obligations. By contrast, in the national settings it is usually held that for want of a better solution, scenario's, ranges and educated guesses should be used to come up with some number (other than zero). We make this point here because the topic of substantive compliance costs indeed leads to the trickiest questions and uneven information. Thirdly, there are some new instruments in the European Better Regulation spectrum where substantive compliance costs are conspicuously missing, such as the One In One Out mechanism and the 25/35 percent reduction drive.

Conversation stopper IV: cross border effects and (other) fragmentation

The positive conclusion of the initial IA regarding the administrative burden of the GDPR was for a major part predicated on cross border effects. The problem of legal fragmentation was declared as solved, and the ensuing reduction of costs of doing business vis-à-vis different DPA's was booked as €2,9 billion. It is remarkable that this dimension is entirely absent from follow-up exercises. It is customary to refer to fragmentation as a problem, but not to calculate it.

In any case, fragmentation has not disappeared, as it is still the most important subject in the two official Evaluation Reports. This can come as no surprise, because the GDPR was characterised as a 'Directive in disguise' from the start, given the many open-ended concepts that it introduced. It was certainly premature to declare the problem of fragmentation as solved, but how it could have been tackled in a more nuanced way is quite a difficult question. Even with the GDPR, which has direct effect as a Regulation and therefore needn't and indeed shouldn't be transposed into national law, many subjects remain for the national legislators, supervisors or administrations to decide. In addition to that, variances in enforcement between Member States are still an important source of fragmentation. These are intrinsic fragmentation factors

which one can work to minimise as much as possible but will never disappear entirely. The solution is not simply to try to ban every kind of discretion at the national level, because even if this was feasible it would not befit the constitutional structure of the EU / Member State legal order. The Dutch Government has for example protested the proposal in the Digital Omnibus that would create one single European entry point for data breach notifications spanning the different Acts that contain such an obligation, stating that this is better dealt with at the national level.[23] Thus, the question of how to assess fragmentation effects in a somewhat empirical but nevertheless proportional way cannot be evaded. The effort made in the original IA was certainly not disproportionate, but not quite empirical either.

A particular kind of fragmentation concerns the uncertainty of interpretations of key GDPR concepts.[24] Even eight years after its full entry into application, an oft-heard complaint is that interpretations can diverge between national DPAs and between DPAs and the European Data Protection Board.[25] Put differently, knowing what exactly the GDPR expects of a business is still a challenge. Typically this complaint is about a lack of practical guidance, not so much of abstract interpretation of GDPR concepts. Nevertheless, the latter can also pose problems. A notorious Dutch dispute concerned the interpretation of "legitimate interests" for personal data processing under point (f) of the first subparagraph of Article 6(1) of the GDPR. The Dutch DPA had – in a move that was immediately widely criticised[26] – from 2019 on taken and enforced the position that purely commercial interests, such as in selling personal data for direct marketing, could never count as such. The business impact (and media exposure) of this stance was obviously very large. This interpretation was quashed by the Court of Justice of the EU almost 5 years after it had been established.[27] It should be noted that the Digital/AI Omnibus still addresses the concern that GDPR concepts have not received sufficient clarification, even after all the years that have passed since its entry into full application.

Conversation stopper V: a carousel of assumptions

In impact assessments, express attention is usually aid to assumptions, and justly so. SCM calculations are simply not exercises that can be rolled out as if everything about them is self-evident. As with all serious analysis, clarity about one's assumptions, interpretations and choices is essential. Of the issues to be tackled in the context of cost calculations, the interpretation of Business-as-usual costs (BAU) is perhaps the most important one. BAU costs don't count towards the regulatory burden, because they represent courses of action that businesses would have taken of their own accord. For instance, the Dutch follow-up assessment mentioned above declared the entirety of costs to ascertain data security to be BAU because any responsible company should be doing this anyway. Without going into that discussion on its merits, we would simply like to point out that IAs with different underlying assumptions are hard to compare at face value. If follow-up exercises are done as if the file was a blank slate and the cues of the Commission are not followed, chances are that the assumptions and outcomes will diverge, as indeed they do. If national officials or the European co-legislators are not satisfied with the assumptions underlying the EU IA, this presents a dilemma. But the solution shouldn't be to simply proclaim one's own assumptions and never look back, because this immediately makes the follow-up exercise less worthwhile.

[23] Eerste Kamer (Dutch Senate), 36890, A.
[24] The issue is discussed here, but could just as well been considered below under 'cost of uncertainty' or 'container concepts'.
[25] See e.g. 'Contribution from the Multistakeholder Expert Group to the Commission 2024 Evaluation of the GDPR', Multistakeholder Expert Group to support the application of Regulation (EU) 2026/679, June 2024.
[26] See e.g. the evaluation 2018-2023 of the Dutch DPA: S. Zouridis, R. Leenes, B.-J. Koops, R. Stolk and P. van der Beek, 'Evaluatie Autoriteit Persoonsgegevens', October 2024.
[27] CJ EU, October 4, 2024, Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens, C-621/22.

Here we would like to introduce a more speculative train of thought that also has a lot to do with assumptions, more specifically those underpinning the SCM model itself. This concerns the cost of intangibles. It is well known that quantifying intangibles on the benefits side is hard to do and often dispensed with. However, intangibles also impact the cost side of the balance sheet: one need only think of the dimension of perceived burdens that come into play where regulation is overly complex or seemingly contradictory. The currency here is perplexity or even stress. In the context of the GDPR, the topical question to ask is what the costs of uncertainty are. The most cited practical problem companies have with the GDPR is that they don't know exactly what is expected of them. This is partly due to the risk-based nature of the regime, which in and of itself was meant to make the obligations more proportional, but definitely has this uncertainty as a side effect for especially smaller firms. In principle, the SCM model implies that these costs cannot be quantified. This is justified and universally accepted because of the inherently subjective element. On the other hand, even if such costs are not quantifiable in their core, the costs of uncertainty do typically translate to decisions by businesses to contract out tasks that they would usually do themselves. Such contracting out does fall within the ambit of the SCM model, namely under the heading of out-of-pocket costs. In the case of the GDPR the practice of contracting out was probably very widespread in the phase when the new obligations had to be implemented in companies for the first time, but perhaps it still amounts to a significant expenditure even now. (We simply don't know.) The lesson to be gleaned here is that the robustness of the assumptions that underpin the calculation of out-of-pocket costs should be a very important consideration in legislative files that are characterised by complexity or uncertainty. We feel that these underpinnings are often not present, which leads to an underestimation of out-of-pocket costs. Conversely, the Digital Omnibus for instance contains a number of references to stress being alleviated by the proposals[28] but leaves it at this qualitative statement without providing further elaboration or evidence.

Conversation stopper VI: underdetermined container obligations and self-assessments

Some obligations are more resistant to ex ante assessment than others. In the GDPR file, but certainly also in other cases where large and complex regimes are in play, two categories of obligations that pose problems stand out. Both categories were left entirely untouched by both the EU IA and the follow-up exercises.

The first category can be called container obligations. By this we mean that it is not evident what a company must do to abide by them, apart from the fact that it seems like a lot. Examples of this in the GDPR are inter alia the obligation to ensure data security, the obligation to adhere to the privacy-by-design principle, and the obligation to ensure data-portability. These obligations are sketched in very general terms in the GDPR and not operationalised to a meaningful extent. This vagueness was certainly already noted at the outset, but in hindsight one can definitively characterise these obligations as having been underdetermined at their launch, as they have years later received their own elaboration and operationalisation in separate legal acts. Data-portability for instance is a major element in the Digital Services Act and has received its own rather elaborate and complex framework there, although the scope of application differs from the GDPR. One can ask the question what the value of the general obligation was, prior to receiving a specific framework. The same can be said of data security prior to NIS2.

The second category concerns the cited risk-based nature of the GDPR. Although this is often not explained, it appears that what is meant by this is mainly the fact that companies are obliged to reach their own conclusions as to the sensitivity of their personal data processing through self-assessments called Data Protection Impact Assessments. If their conclusion is that these risks are present, a stricter GDPR regime kicks in. As such this self-assessment is far from gratuitous because there can be major consequences if the

[28] The Common Agricultural Policy Omnibus (package number 3) is an even clearer example of this (COM (2025) 236 and SWD (2025) 236).

DPA disagrees. From a cost perspective, obligations such as these are very difficult to assess ex ante. And they are notoriously difficult for smaller companies, who often revert to contracting this exercise out even if no operational risks are apparent. As we already noted, the extent of contracting out merits more robust ex ante scrutiny.

Conversation stopper VII: unaccounted for (but very costly) policy shifts

There is one dimension of costs that was negated by the EU IA and ignored in the follow-up exercises but is nevertheless prominent in the public eye. That is the dimension of costs for private individuals, which are incurred when one for instance wants to post pictures of a birthday party on social media. As such self-broadcasting is considered as sending something to the wide world, it is personal data processing for the purposes of the GDPR, which means that in principle consent needs to be sought from all parties concerned. In technical terms, this is about the ambit of the so called 'household exception'. The original IA stated that self-broadcasting shouldn't be covered by the GDPR, but this position didn't survive the ensuing negotiations. As the IAs are not updated during the EU decision making process, such a fundamental departure does not lead to any revision of the assessment.

While this essay does not primarily deal with costs to citizens, this disparity between the IA and the Regulation that was eventually adopted does merit attention. As noted by many, the fact that the European Parliament and the Council generally do not perform IAs on their amendments, and that the Commission does not want to take responsibility for reassessing the negotiation result, presents quite a substantial leakage in the Better Regulation system. Sometimes there are even disparities between the IA and the actual Commission proposal, published on the same day and under the same authority.[29] In order for EU IAs to be less of a one-off exercise, a way needs to be found to close the loop, certainly as regards the European decision-making phase, but ideally also in view of experiences on the ground once the Act has entered into force.

Conclusions and agenda

This essay points to avenues to make the assessment of costs of EU legislation more integrated in policy development, deliberation and upkeep. The case of the GDPR presents a strange coincidence of on the one hand a very prominent file that has seen many discussions on practical implications, but on the other hand an enduring near-complete enigma as to the quantitative regulatory burden. Closing the loops within the European decision-making process, but also in the aftermath when the facts on the ground become clear, could go a long way towards strengthening the conversation on the costs of EU legislation. The calculation of regulatory burdens merits a more sustained and transparent effort, seeing how much weight simplification now carries. If EU and Member State calculations could become more mutually reinforcing, instead of being one-off, disparate exercises, we would be all the wiser. A simplification drive such as the Digital Omnibus that is not founded on a common understanding of what we as societies are paying, risks stirring up more confusion than necessary.

[29] E.g. concerning the Industrial Accelerator Act, compare COM(2026)100 and SWD(2026)71 as regards the sectors covered.