Data & More | The cost of doing nothing

Protecting digital privacy and minimizing the risk, cost, and liability of processing unstructured data

"The only thing necessary for the triumph of evil is for good men to do nothing."
— Edmund Burke

Table of contents

Table of contents **1**

Executive Summary **2**

Why inaction is a liability **3**

The Good - Being audited by a Data Protection Authority. 5

The Bad - The risk of a dirty data breach caused by third-party bad actors (hacking) 7

The Ugly - Whistle blowers & bad leavers 12

Business Case Framework **13**

Summary **16**

Executive Summary

The cost of not deleting illegal privacy data can be defined as the **Data Privacy Risk Premium**. The risk premium is calculated as the likelihood of an adverse event times the cost of the event. Put another way, it is the yearly amount an organization should allocate to cover the expense of retaining illegal Privacy Data instead of deleting it.

The Data Privacy Risk Premium aggregates different risk factors, such as **Legal risk**, **Reputational risk**, and **Operational risk**. There are many more, but these are the big ones. By analyzing the literature and the events in 2024, we have established the following risk premium as suggested by the **European Data Protection Board** and industry leaders in the field. Detailed references are available in the relevant sections.

	Legal Risk Premium	Reputational Risk Premium	Operational Risk Premium	Data Privacy Risk Premium
As a % of global revenue per year	0,28%	0,21%	1,20%	**1,69%**
As a cost pr. employee per year	€280	€210,00	€3.375	€3.865
As a cost of a non-compliant document	€0,71	€0,53	€9	**€10**

For a total **Data Privacy Risk Premium** 1,69% of global turnover per year.

The Data Privacy Risk Premium is a function of the amount of Personal Data stored. If you know the total number of privacy documents, the most accurate price estimation is calculated using the cost per document. If not, the number of employees or global turnover can be used, but it must be indexed by industry to be reasonably accurate.

Industries with small amounts of personal data, like retail, are indexed at 55%, and professional services, which have a high density of personnel, are indexed at 222%, which adjusts the Data Privacy Risk Premium for retail to 0,93% and 3,75% for professional services. Find index on pager (15)

The events underpinning the Data Risk Premium are being audited by the data protection authorities, having a dirty data breach due to third party's bad actors, or having insiders use non-compliance as a bragging chip.

Why inaction is a liability

Failing to delete personal data you no longer have a legitimate interest in is not a neutral decision. In Denmark and many other EU countries, it's a legal requirement, and failing to comply can lead to fines and, in some cases, criminal prosecution.

You might get away with it—but so might someone committing fraud or skipping taxes—until they don't. The **Danish Data Protection Act (Act No. 502 of 23 May 2018) — specifically Section 41** — outlines the circumstances under which violations may constitute criminal offenses. One of the most common grounds is acting in bad faith or demonstrating gross negligence in failing to delete illegally held data.

If the data protection agency identifies a bad actor, the costs are not just legal—they're reputational, operational, and sometimes personal.

Ironically, being audited by the Data Protection Authorities can turn out to be a "good case." There are bad and truly ugly cases ahead for organizations that are in bad faith and neglect to clean up illegally held private data. - *We will get back to the bad and the ugly cases.*

Let's start by reminding ourselves why we deleted the personal data we no longer have a legitimate interest in.

We delete personal data to
protect the people who trusted us
with their data in the first place.

Now, **doing the right thing seldom makes it to a business case**, so let's examine the actual financial risks, their impact, and the cost of mitigation.

When using risk in a business case, you must first find the **Risk Premium**, which is calculated as the probability of the event occurring in a given time - times the cost of the impact. In other words, the likelihood of the event times the cost of the event.

Then, you can use the Risk Premium to compare with the risk mitigation. In this case, the cost of implementing automatic data compliance that deletes illegal documents vs the risk premium of the data that would otherwise be deleted

To keep it simple, if, for example, the probability of being hacked is 4% per year and the cost of the breach for the specific organization is €5 million, the Risk Premium of keeping data is 4% of €5 million = Data Privacy Risk Premium is €200.000 per Year.

There are at least three significant risks associated with keeping unstructured privacy data such as we find in mail files, SharePoint, and onedrive, which derives the Data Privacy Risk Premium:

Legal Risk: The legal risk is mostly fines and, in rare cases, the legal cost of personal litigation

Reputational Risk: The main reputational risks are lost revenue and a drop in share prices

Operational Risk: Operational risks are closely tied to the actual event and include the direct cost of employees, the cost of special consultants, and the infrastructure needed to alleviate the event.

To uncover legal, reputational, and operational risks, we must investigate under what scenarios they actually exist. For this, we will use three different scenarios organizations that are collecting and processing unstructured privacy data can find themselves in.

The Good - This risk of being audited by a Data Protection Authority

The Bad - The risk of a dirty data breach caused by third-party actors

The Ugly - The risk of a bad leaver using GDPR as extortion

The Good - Being audited by a Data Protection Authority.

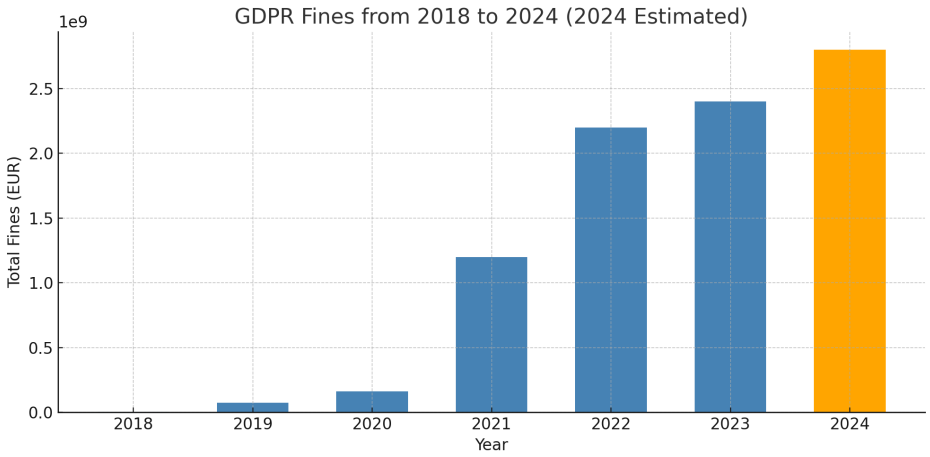
This is a good scenario because all organizations should be able to pass an audit by the DPA - thereby documenting for all stakeholders that your organization lives up to its responsibilities and takes Data Protection seriously.

Calculating the Legal Risk Premium

According to the GDPR enforcement tracker, in 2024, about 500 companies were fined for Data Privacy violations in the EU, and an estimated 4,300 companies were investigated based on data from the European Data Protection Supervisor (EDPS). The majority had over 250 employees, of which the EU has 64,000.

So, if you have more than 250 employees and illegal data, which we assume the audit identified, the probability of being fined is 4300 / 64.000 = 7% pr. year.

Now, the price of being fined 4% of global turnover appears quite substantial, and their fines are increasing (the estimate for 2024 is 2.8 billion euros when everything settles, with 1.4 billion already agreed for 2024). **However, the actual fines per company are about 0.4% of global turnover and not the 4%** that is the legal limit for the fines.



(Source:https://www.enforcementtracker.com/ & www.itgovernance.eu)

If we **reduce the legal risk** only to GDPR fines, based on the above metrics, the probability of a fine is about 7% per year (EU companies) and 0.4% of global turnover. In this case, we leave out the risk of personal litigation - which, in the end, is not a risk for the organization.

The Legal Risk Premium for having dirty privacy data is 7% multiplied by 0.4%, resulting in 0.28% of the organization's global turnover per year.

We can find the Legal Risk Premium by employee by multiplying the average EU turnover per employee (€100.000) by the Legal Risk Premium as expressed as a percentage of global turnover (0,28%), which equals €280 per year.

We know that for the Data & More Global Privacy Classification, the average number of privacy data per employee is 397 (with a variance between 180 and 880), which, when divided by the Legal Risk Premium (€280), is € 0,71 per document per year.

But even though the fines can be significant, they're only one of the first impacts; the second impact is Reputational damage, which, in a business case model, is represented by the Reputation Risk Premium.

The **Reputational Risk Premium** is calculated as the probability of the event—which in this, the Good Case, is the same as the probability of being audited per year) X (reduction in turnover) + (reduction in share prices)

A study by the Centre for Economic Policy Research (CEPR) found that companies exposed to the GDPR experienced an average 2% decrease in sales and an 8% reduction in profits.

A study published in *Information and Computer Security by Ford et. al. 2023* analyzed 25 GDPR fine announcements and found statistically significant cumulative abnormal returns averaging around 1% up to three days after the announcement. In many cases, the negative impact on market value exceeded the monetary value of the fine itself, indicating that even

relatively minor fines could result in substantial market valuation losses for companies, regardless of their market capitalization.

We can now calculate the Reputational Risk Premium with the following Probability of audit 7% | Cost in turnover 2% | Reduction in share price 1%.

The Reputational Risk Premium for having dirty privacy data in an audit is 7% multiplied by (2% +1%), resulting in 0.21% of the organization's global turnover per year.

The Bad - The risk of a dirty data breach caused by third-party bad actors (hacking)

The really bad scenario is that the stolen data is dirty, i.e., it contains information that the organizations should have deleted long ago. Hackers are very good at spotting dirty data, and it gives them considerable leverage in any negotiations.

Many professional hackers are state-sponsored by countries such as North Korea, Russia, and China and are strong negotiators. They often achieve a ransom of 25% of annual turnover for smaller companies and about 5-10% for larger enterprises.

The numbers vary a lot depending on the industry, the privacy data in question, and if the hackers manage to encrypt the data sources as well.

Now, the evil thing about dirty data breaches is that you will have to report them to the Data Protection Authorities, whose first act will be to investigate why you have dirty data in the first place - which brings you back to square one.

Now, companies can survive a bad audit. Still, data breaches resulting in millions of privacy documents ending up is a reputational catastrophe that can put the company at risk and ruin

the management via liability claims. The latest example is the company 23andMe, which had a Data Breach in 2023 and has just filed for bankruptcy. The CEO, Anne Wojcicki, faces numerous ongoing personal lawsuits for gross negligence.

March 24 (Reuters) - 23andMe (ME.O) on Sunday filed for bankruptcy in the U.S. after struggling with weak demand for its ancestry testing kits and a 2023 data breach that damaged its reputation

Let's sum up the cost of a dirty data breach.

1. Operational cost from IT, manager, and third party consultant. The average cost in the event of a ransomware/data breach is **€170 per file containing personal data** (https://www.ibm.com/reports/data-breach)
2. Ransom payments to hackers (optional, but refusing to pay the ransom can increase the brand damage. Form **5-25%** of turnover
3. Fines imposed by the data protection authorities average € 50,000 and € 2,500 in compensation to data subjects. (In several rulings, the EU has set the costs of compensating individuals whose data has not been properly handled at €2,500 per person.) On average, this cost is 0.4% of global turnover
4. The reputational damage we know in the example above varies significantly from 1-2% of global turnover to an extinction-level event. For the business case, we will use 3% as suggested by CERP and Ford et. al. 2023

To calculate the **Operational Risk Premium** arising from hacking, we need to identify the average number of documents at risk. Based on Data & More global statistics, we have the following insights.

Industry	Avg. Privacy Documents per Employee
Technology	300
Healthcare	280
Finance	750
Retail	220
Manufacturing	180
Real Estate	400

Transportation & Logistics	220
Energy & Utilities	330
Education	440
Public	370
Professional Services	880
Average numbers	**397**

In order to calculate the organisation's impact, we have to take the number of privacy documents produced per employees are 397 documents, times the average cost per breach document, which is 170€ (https://www.ibm.com/reports/data-breach) which gives **67.490€ in operational value at risk pr. employee**.

The operational **value at risk per employee must then be discounted by the probability of being hacked per year.**

The risk of being hacked

If we start with the risk of being hacked, we have some varying numbers by different sources

- According to Sjoerd Langkemper 2019 the risk of a company getting hacked is around 1% yearly.
- Eye Security 2023 suggests that businesses have a 1 in 5 chance of a data breach caused by hacking.
- According to IBM's Cost of a Data Breach Report 2023, 83% of organizations have experienced more than one data breach, and based on historical trends, the probability of a company experiencing a data breach within two years is estimated at 27.7%.

For this business case, we will use the 83% discount over 15 years, which is estimated at 5% per year. This number is higher than Sjoerd Langkemper 2019 but lower than Eye Security 2023, which takes the heightened security risk somewhat into account.

The Operation Risk Premium as a percentage of global turnover is then €1.221 (the Operational Risk Premium pr. employee) divided by €100.000 (the average employee global turnover) Which equals 1.2% per year.

If we want the Operations Risk Premium per year, we have the (the number of documents per employee 397) times the cost €170 divided by the probability of being hacked. 5%, and we have €3.374 per employee per year.

If we want to identify the value of cleaning up the data - separate from the breach itself we can do a side-by-side analysis.

Below is a **side-by-side** comparison of estimated costs for a **100,000-privacy** data breach under two scenarios from a mid-size SaaS company.

1. **"Dirty Data"**: The company **did not** have a legitimate interest or lawful basis for storing these passports (heightened regulatory risk, including fines).
2. **"Legitimate Interest"**: The company had a **valid legal basis** (e.g., compliance, contractual necessity) for holding the passport data (we assume **no regulatory fines** here) and all dirty data have been removed.

Both scenarios assume the same scale (100,000 privacy documents) but differ primarily in **regulatory fines** and **legal costs**.

We assume that the company did NOT pay any ransom to the hackers.

Note that all figures are rough estimates to illustrate potential differences.

For detailed analyses of the assumptions and methodology, please see Appendix 1 and Appendix 2.

Cost Component	"Dirty Data" (No Lawful Basis)	"Legitimate Interest" (Lawful Basis)	Δ (Difference)
1. Per-Record Cost (Investigation, response, and indirect costs)	$15M–$18M *(\$150–\$180 × 100,000)*	$15M–$18M *(Same base cost for as non lawful)*	$0
2. Regulatory Fines	$5M–$15M+ *(Heightened due to illegitimate processing under GDPR, etc.)*	$0 *(No fines assumed if fully compliant / legitimate interest)*	$5M–$15M
3. Notification & Remediation (Identity monitoring, call centers, mailings)	$2M–$3M	$2M–$3M	$0
4. Legal & Litigation Costs (Lawsuits, settlements, legal fees)	$2M–$7M *(Higher risk if regulators or class actions allege unlawful data retention)*	$1M–$2M *(Still possible lawsuits, but less regulatory leverage)*	$1M–$5M

Cost Component	"Dirty Data" (No Lawful Basis)	"Legitimate Interest" (Lawful Basis)	Δ (Difference)
5. Security & Infrastructure	$1M+	$1M+	~$0M (similar)
6. Reputational Damage & Churn (Brand impact, PR, lost revenue)	$5-$6M *(Possibly heightened if deemed bad faith)*	$1M+	~$4M
Potential Overall Range	**$30M–$50M+** *(or more, if fines and lawsuits escalate)*	**20–$25M+** *(no regulatory fines, reduced legal costs)*	**$10M–$25M+** difference ~45%

The key takeaway is that the on average the cost of a data breach is reduced by 45% if the data is clean.

The Ugly - Whistle blowers & bad leavers

Whistelblovers
Data leaks happen all the time, but the majority are not reported, even though it's a legal requirement. The Data Protection Authority's whistleblower system is the number one source of data leak investigations. However, the trend is clear: Combining unhappy employees with bad privacy management is an accident waiting to happen.

Bad leavers
The majority of Data Subject access requests that Data & More Data Subject managers process are investigations required by former employees. These requests are often sparked by a data subject using GDPR to gain leverage during the negotiation or court case that arises as a result of the individual leaving the organization.

Now, it is challenging to take whistle-blowers or bad leavers directly into the business case, but if the company has many such cases, the legal and reputations risk must be adjusted upward, increasing the overall **Data Privacy Risk Premium.)**

Business Case Framework

As this paper clearly states, the cost of doing nothing—a "we will just pay the fines" approach—is not an option. **It is illegal. Deleting illegal data puts people who trust you in danger and can be life-threatening to your organization.** So, a business case must be built on how you choose to delete your illegal privacy data as an alternative to doing nothing and then set in perspective of the three scenarios happening: "the good, the bad, and the ugly."

A valid business case for deleting illegal data must, therefore, have two conditions.

1. **The cost of doing nothing**. Since we are dealing with risk, we must reduce all risks to a risk premium, in this case, the "**Data Privacy Risk Premium**." The good way to think about the Data Privacy Risk Premium is the cost of insurance—or what it would cost to insure the company against the risks outlined in the good, bad, and ugly scenarios.

2. **The cost of doing something**. Automatic Data Complicae is the most secure way of deleting Illegal Data, but some organizations have tried manual cleanup or Microsoft Purview to remove Privacy Data.. It is important to stress that neither **manual cleanup**

nor MS Purview has any practical effect or impact on the risk because it simply does not work.[1]. However, it provides a thin layer of plausible denials that might save the executives from some legal action and reduce the fines.

To create the business class case, use the metrics below to calculate the Data Privacy Risk Premium.

	Legal Risk Premium	Reputational Risk Premium	Operational Risk Premium	Data Privacy Risk Premium
As a percentage of global revenue per year	0,28%	0,21%	1,20%	1,69%
As a cost pr. employee pr. year	€280	€210,00	€3.374	€3.864
As a cost of a non-compliant document	€0,71	€0,53	€9	€10

Then, index your risk based on the industry or, if you have a PoC, estimate how many documents you have. Using the graph below

Industry	Index
Technology	76%
Healthcare	70%
Finance	189%
Retail	55%
Manufacturing	45%
Real Estate	101%
Transportation & Logistics	55%
Energy & Utilities	83%
Education	111%
Public	93%
Professional Services	222%

[1]Data & More has analyzed hundreds of thousands of datasets that should have been manually cleaned or protected using Microsoft Purview—and found no significant difference compared to taking no action at all.

Now, the Data Privacy Risk Premium calculations depend on which of the metrics you are following. This is because the organization is calculated as the business case from deviating from the mean. So, if you have fewer privacy documents than average, the number will be less. Calculate the Data Privacy Risk Premium by documents rather than a percentage of global turnover.

Business case: Retail Company

The number of employees is 7.000, which gives a Data Privacy Risk Premium per year of (7.000 X €3.865) *55% = 14.8 million per year.

The cost of implementing an automated compliance system like Data & More is 153.000 euro - according to dataamore.com, which has a net positive impact of 1€4,8 mill. minus 4150 thousand equals **14.65 mill. A positive business case per year.**

In the case that the organisation's IT department has such high standards that they don't believe they will be hacked in the next 15 years, we can take away the operations part of the Data Privacy Risk Premium and focus on the legal (€280 user/year) and reputation (€210) risk which gives Data Privacy Risk Premium. (7000* (280+210))*55% = €1.886.500 and with the cost of the automatic data compliance says €153.000 is still **a very compelling business case** with a return of €1.732.500 mill. a year.

Summary

We have identified a significant financial risk associated with the retention of illegal privacy data, which we have termed the "**Data Privacy Risk Premium**." This risk premium encompasses legal, reputational, and operational risks and can be quantified as a percentage of global revenue, cost per employee, or cost per non-compliant document. Through analysis of European Data Protection Board guidelines, industry experts, and industry data from 2024, we have established a Data Privacy Risk Premium of 1.69% of global turnover per year. This figure is derived from a combination of legal risk (0.28%), reputational risk (0.21%), and operational risk (1.20%).

Furthermore, our analysis indicates that the Data Privacy Risk Premium varies by industry, with indices ranging from 55% for retail to 222% for professional services, reflecting the differing densities of personal data processed. We have examined three potential scenarios: regulatory audits, data breaches, and insider threats, each carrying distinct financial and reputational implications. Specifically, data breaches involving "dirty data" (data that should have been deleted) pose substantial risks, including significant operational costs, ransom payments, regulatory fines, and severe reputational damage, potentially leading to bankruptcy and personal liability for management.

Based on our analysis, we conclude that inaction regarding the deletion of illegal privacy data constitutes a substantial financial and legal liability. **The Data Privacy Risk Premium is not negligible and should be considered a critical operational cost**. We have demonstrated that the implementation of automatic data compliance systems offers a viable mitigation strategy, significantly reducing the risks and costs associated with data breaches and regulatory scrutiny. The business case framework we have developed illustrates the potential return on investment in such systems, highlighting the financial prudence of proactive data management. In essence, our findings underscore the necessity of a strategic shift from reactive to proactive data governance to safeguard organizational integrity and financial stability.