University of St.Gallen
Institute for Media
and Communications Management

# Data Protection in Swiss Law Firms

Research Report

University of St.Gallen, St.Gallen, 12. September 2022

University of St.Gallen

Institute for Media
and Communications Management

Conducted by
Chair of Media and Culture,
Institute for Media and Communications Management (MCM),
University of St.Gallen (HSG)

Prof. Dr. Veronica Barassi
Kimberley Kernbach
Rahi Patra

Funded by
Innosuisse Innovationcheck

In collaboration
with ARCANO / Codefour GmbH

St.Gallen, 12. September 2022

# Table of Contents

1 Introduction 1

2 Research Project 3

2.1 Research Method 3

2.2 Sample Description and Recruitment 4

2.2.1 Characterization of Survey Participants 4

2.2.2 Characterization of Represented Law Firms 5

3 Data Protection in Swiss Law Firms: Findings and Analysis 7

3.1 Changing Awareness of Data Protection amongst Swiss Law Practitioners 7

3.2 Data Protection: Beliefs, Attitudes and Room for Improvement 9

3.3 The Key Challenges to Data Protection in Swiss Law Firms 12

4 Strategies and Solutions for Data Protection in the Legal Sector 14

4.1 Data Protection Training and Literacy: How can we Improve? 14

4.2 File Sharing, Vulnerabilities and Legal Technology Solutions 17

5 Conclusions 23

References 25

List of Abbreviations 27

List of Figures 27

# 1 Introduction

In the legal sector data protection has always been crucial. Legally (and ethically), it is the lawyer's duty to protect the client's privacy and confidentiality. According to **Art. 15 of the Swiss professional ethics by the Swiss Bar Association** (Schweizerische Standesregeln des Schweizerischen Anwaltsverbands, SAV): *"Lawyers are subject to professional secrecy for an unlimited time and towards anyone on everything that has been entrusted to them by clients as a result of their profession. […] They shall ensure that professional secrecy is maintained by their staff, employees and other auxiliary persons."* A violation of the legal provision to professional secrecy may thus by punished by the Swiss Criminal Law Art. 321 StGB.

Whilst data protection and client's privacy have always been important for the legal sector, today data protection has become a fundamental challenge for Swiss law firms for two main reasons. On the one hand, we have seen the introduction of new regulatory frameworks that are having a direct impact on the data protection practices and strategies of firms. The **General Data Protection Regulation** (GDPR), for instance, has been implemented by the European Union (EU) and the European Economic Area (EEA) in 2018. The EU is also currently working on the implementation of the **ePrivacy Regulation** (ePR) as lex specialis to the GDPR, which is supposed to repeal the Privacy and Electronic Communications Directive 2002. It specifies data protection on the Internet and within electronic communication. The regulation is still under review in the European Parliament and is not expected to enter into force before 2023 (CMS Legal, 2022). Such regulatory frameworks have been adopted by a revised Swiss data protection law (Datenschutzgesetz, DSG), called **E-DSG** (Entwurf des Datenschutzgesetzes) or **nDSG** (neues Datenschutzgesetz). [1] The proposal has been accepted by the federal council in September 2020 and will come into force by September 2023 (Gross, 2022).

On the other hand, law firms are increasingly exposed to cyber-attacks and data breaches. According to the Legal Technology Survey Report of the American Bar Association, in 2021, the reported percentage of firms experiencing a breach ranged from 17% of solos and firms with 2-9 attorneys, about 35% for firms with 10-49, 46% with 50-99, and about 35% with 100+. Data breaches can have a significant impact on law firms. Clients will leave law firms where they feel that their personal information is not secure. According to the 2019 Cost of Data Breach Study by IBM Security/Ponemon Institute, the average total cost of a data breach has increased by 1.6% from the previous year and 12% over the past 5 years. Data breach now costs businesses an average of $3.92 million. The average size of a breach is 25,575 records containing sensitive and confidential information. Each record costs about $150 on average globally. (Fischer, 2020)

Despite data protection is becoming a fundamental challenge for the legal sector in Switzerland, the state of research on legal practitioners and everyday data practices is still widely underdeveloped. Some have highlighted the need for compliance to data protection regulations

[1] The revised DSG may either referred to by E-DSG or nDSG: For E-DSG see for example: https://www.pwc.ch/de/publications/2018/E-DSG_Revision-des-Schweizer-Datenschutzgesetzes.pdf; for nDSG see for example: https://www.axa.ch/de/unternehmenskunden/blog/sicherheit-und-recht/recht-und-justiz/neues-datenschutzgesetz.html

in several areas of the economy and the law sector in particular (Ng, 2020; Fischer 2020, Zhang 2020) or have provided guidance in the complex field of data protection regulations (Cepero, 2020; Matich, 2021; Wolters Kluwer 2017; Zhang, 2020). Others have identified the increased risk of cyberthreats and attacks to legal data by showing how this risk has been amplified after the Covid-19 pandemic by home office practices (Tillay, 2021; Nabe 2020). However, while some research can be found that discusses issues of data protection in regard to Swiss companies in general (PwC, 2018; Patklom, 2018), we still lack a critical and in-depth understanding of the problems that emerge in everyday practice for Swiss law firms, how Swiss legal practitioners are dealing with the problems of data protection, or what they think about existing legal technology solutions.

This research project was designed to give voice to the day-to-day experiences, beliefs and practices of legal practitioners in Switzerland. Its aim was to gain a more nuanced knowledge of the potential issues, challenges and constrains that define data protection practices amongst legal practitioners in Switzerland and to explore how Swiss law practitioners currently deal with raised standards of privacy and security at the international and national level, how they manage these issues in their day-to-day working life, and what solutions they envisage. It is important to point out that this research project has been designed to be exploratory in nature and shed light on the practices, beliefs, misconceptions, and challenges that law practitioners face in their everyday work life; it was not aimed at assessing whether law firms are currently complying with data protection regulations.

The project was conducted by the Chair of Media and Culture at the Institute of Media and Communication Management at the University of St. Gallen (MCM-HSG). Funding for the project was granted by the Innosuisse Innovationcheck thanks to a collaboration between the Chair of Media and Culture at the MCM-HSG and ARCANO, a Swiss Privacy by Design legal technology file sharing solution company, who was interested in understanding the issue of data protection in Swiss law firms more in-depth. The research project was designed and carried out exclusively by the academic partner in full compliance with research independence and excellence. It is for this reason that the results of the research are open access and aimed at the legal sector in general, the public, as well as those interested in acquiring an in-depth understanding of everyday practices and challenges when developing legal technology solutions.

# 2 Research Project

## 2.1 Research Method

The results presented in this report have been gathered via an online survey amongst Swiss legal practitioners, which was carried out over a period of three months between February 2022 and May 2022. The survey was based on a mix-method approach and combined quantitative questions with open ended qualitative questions. Our approach thus was based on a strong qualitative component, which is essential to gain a more in-depth and critical understanding of everyday beliefs, practices, and challenges. Because of the qualitative dimension of the project our aim was to keep the number of survey participants between 50 and 100. The survey focused on four areas of investigation:

Understandings of Data Protection and Regulations

How aware are legal practitioners of data privacy regulations and security risks? How much do they know about data protection regulations? How confident do they feel about their everyday data protection practices?

Data Protection and File Sharing Practices

What are the day-to-day practices and behavioural patterns of data sharing amongst legal practitioners? What technologies and strategies are used? In which way? How useful are these technologies?

Data Training Experience and Literacy

How far do legal practitioners feel that they have received sufficient training? How much training did they receive? Did the training made them feel more confident in their data protection practices?

Understandings of Legal Technology Solutions such as Privacy by Design[2] or Default[3]

How would legal practitioners feel if their firm used Privacy by Design/Privacy by Default (PbD) technologies? Have they ever used Privacy by Design? How was their experience?

At the beginning of the survey respondents were asked to provide few general and anonymized details such as: **area of law they practiced, role in the firm, and stage of career**. Because of the

[2] *Privacy by Design* refers to ensuring that privacy and data protection are in-built into the design of the system, service, product, or process through appropriate technical and organizational measures. E.g., a software that anonymizes faces in videos to safeguard privacy.

[3] *Privacy by Default* refers to ensuring that only the necessary data is processed to achieve a specific purpose so that, by default personal/sensitive data is not made accessible publicly. E.g., websites prompting for user consent before any cookies are allowed.

highly sensitive field of investigation the survey relied on general and anonymized research questions. **The data has been anonymized and no firms or individuals will be identified** in this report in compliance with our informed consent form. To be inclusive of all language areas in Switzerland the survey was conducted in English language. The online survey has been created via the survey tool Unipark.

## 2.2 Sample Description and Recruitment

To partake in the survey participants had to be employed in a Swiss law firm or work as an individual lawyer in Switzerland. All cantons and language areas of Switzerland have been included. The participation in the survey was not limited to lawyers, but we also included law firm employees working in supportive functions, whose file sharing practices are believed to have a similar important impact on the whole law firm's data protection effectiveness.

The approached law firms have been identified via a public listing provided by the Swiss Bar Association. In total, 344 Swiss law firms (accounting for 1199 email individual contacts) have been contacted via email. To contact the law firms, email addresses have been retrieved from the firm's websites. Further, additional recruitment strategies involved a survey distribution via several law networks and communities accounting for over 3000 contacts (e.g. Newsletters by HSG Law Alumni or Zürcher Anwaltsverband). Further, referrals within the researchers' network have been used to recruit more participants. We approached each law firm with the request to limit the participation within the firm to max. 4 people to avoid bias (e.g. one law firm having more individuals participating).

In total, the survey was distributed to over 4000 Swiss law practitioners. Thus, 160 participants have been recruited and 77 participants have successfully completed the survey. This number fell comfortably within the range of our proposed sample target (min. 50 – max. 100) that is suitable for a mix-method approach which focused on a qualitative dimension.

The recruiting process has been particularly difficult for the research team and this we believe is in itself a very important finding on the state of data protection in Swiss Law firms. In fact, we were approached by different participants who have admitted that they did not want to participate to the survey due to the sensitive field of inquiry and on one occasion we have also been told that our recruitment problems reflected the fact that the research project touched upon the "**Achille's heel" of law firms**.

### 2.2.1 Characterization of Survey Participants

More than three quarters (86%) of the sample participants were employed in positions directly related to practicing law. This included partners (64%), practicing lawyers (18%) and paralegals or assistant lawyers (4%) (see figure 1, left). It is noteworthy that a striking majority (78%) of all participants indicated to be part of the decision-making progress when it came to the employment of IT tools within the law firm (see figure 1, right). Only a relatively small share of the sample (14%) was employed in supportive functions such as: office management (9%), Backoffice positions as HR, Controlling or IT (4%) or other functions (1%). Hence **the results of this survey are more reflective of law partners or individuals who belong to the decision-making** process when it comes to implementing legal technology solutions.

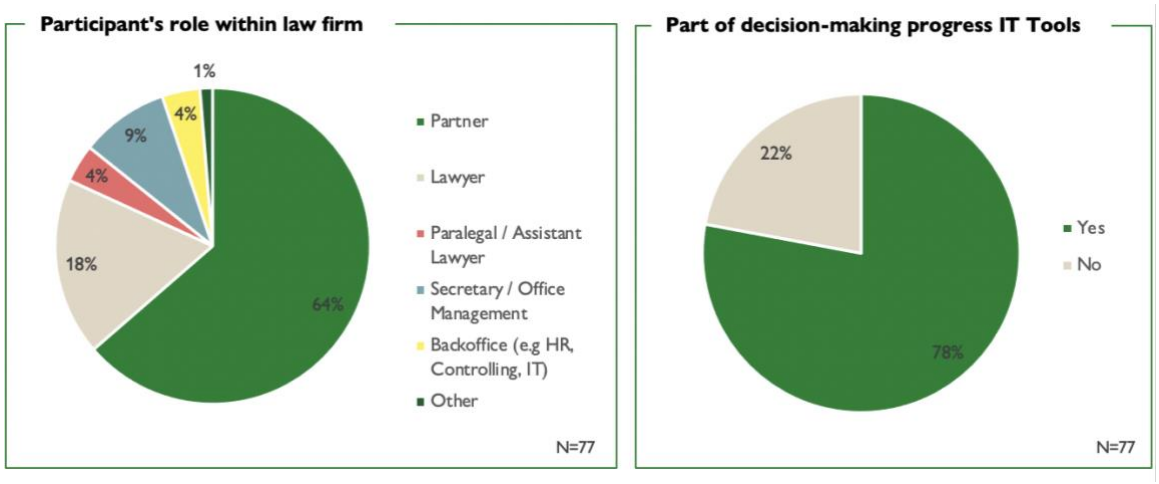


Figure 1: Participant's characterization within law firm

### 2.2.2 Characterization of Represented Law Firms

The law firms represented by the participants in the survey went **from small to medium and big sized law firms** with a relatively fair distribution among all sizes. 21% of the participants indicated to be working for a big sized law firm with more than 100 employees, 42% indicated that they were working for medium sized firms which ranged between 10 and 100 employees (11-50 employees: 39% / 51-100 employees: 3%) and 35% were working for small sized law firms (≤ 10 employees: 35%). A small minority of 3% indicated to work as self-employed individuals.[4] (see figure 2, top left)

As the survey was distributed among all cantons in Switzerland the represented law firms **cover different Swiss language areas**. With an overwhelming majority (92,2 %) of the represented law firms serving in (Swiss) German speaking areas and relatively smaller shares of law firms that participated to the project serving in the French speaking area (16,9%) or the Italian speaking area (3,9%).[5] Although (Swiss) German seems to be overrepresented, the present allocation among the different language areas only parallels the effective distribution of the spoken national languages among Switzerland, which is 62,6% German speaking, 22,9 French speaking, 8,2% Italian speaking and 0,5% Romansh speaking (Official Website of the Swiss Government, eda.admin.ch). (see figure 2, top right)

The participants recruited worked in law firms which covered **different fields of law**: civil law (70,1%), criminal law (46,1%), public law (53,2%), family law (40,3%), tax and duty law (26,0%), and commercial law (62,3%).[6] As the fair distribution between civil and commercial suggests, the represented law firms served both kind of clients: i.e., business and private clients (78%). The remaining 22% almost equally spread across serving only business clients (i.e., companies, corporations, or institutions; 13%) or serving only private clients (i.e., private individuals; 9%). (see figure 2, bottom)

[4] Note: The total sum exceeds 100% due to mathematical rounding. See figure 2 for exact percentages including decimals.
[5] Note: Since some law firms are offering their service in several Swiss language areas, multiple entries have been possible, and the total sum exceeds 100%.
[6] Note: The percentages indicated reflect the share of represented law firms that are actively serving that field of law.

The distribution regarding size of law firm, language areas, field(s) of law and clients to be served reveal that the insights provided by this survey stem from participants representing insights of law firms with different backgrounds and thus assure to provide multiple points of view that are not tied to a certain group of law firms.

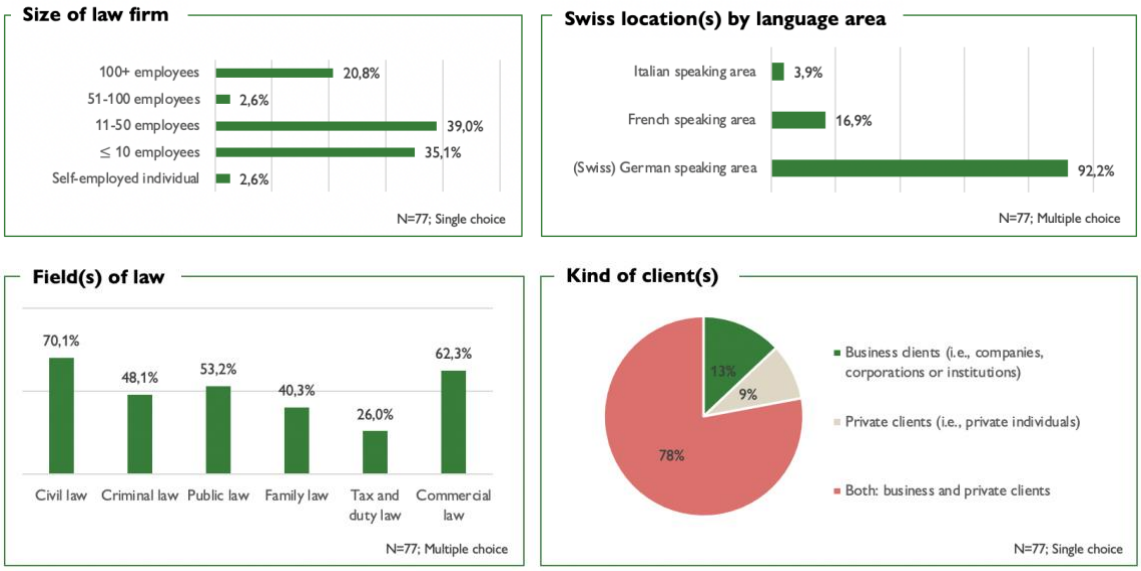


Figure 2: Characterization of represented law firms

In the survey we were interested in the understanding of whether firms operated across different offices or borders. As shown in figure 3, the insights reveal that indeed most firms were working with offices or clients across different locations or nationalities. 48% of the represented law firms operate across several offices in Switzerland (see figure 3, left). A small but not unnoticeable share of 14% of the law firms have additional offices located outside of Switzerland – either in the EU (8%) or worldwide (6%) (see figure 3, middle). An overwhelming majority of firms (83%) also revealed that they would serve international clients (see figure 3, right).

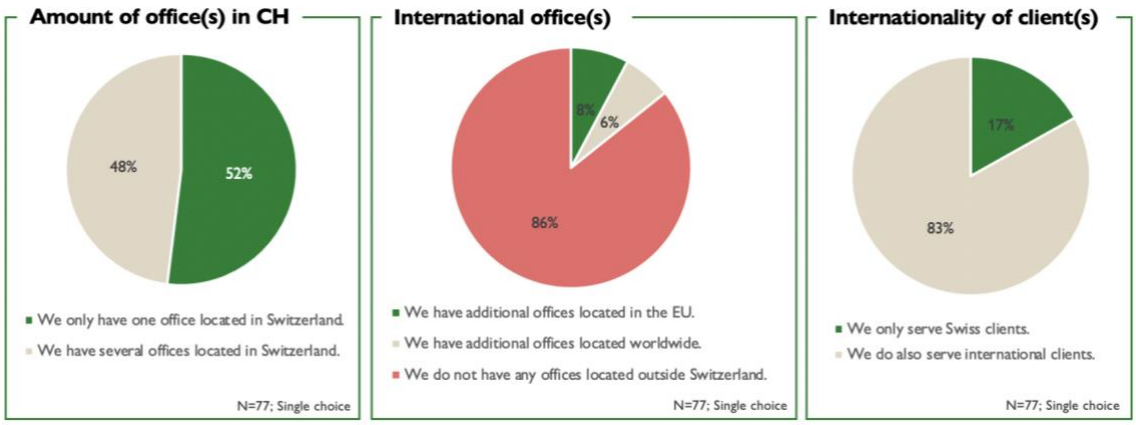


Figure 3: Office structure and client's internationality of represented law firms

# 3 Data Protection in Swiss Law Firms: Findings and Analysis

## 3.1 Changing Awareness of Data Protection amongst Swiss Law Practitioners

Data protection is a fundamental professional value for Swiss law practitioners. Our respondents believed that **data protection was tightly interrelated to their duty of professional secrecy**. Respondents commented that protecting their clients' privacy and secrecy was not only demanded "by law" but was also an "[e]ssential part of [their] professional activity" or even the "foundation of lawyer's work". Yet they also argued that data protection was acquiring a new importance as it needed to be understood with reference to the rapidly changing digital environments in which "sensitive data [is] increasingly being transferred online". They also believed that the new importance of data protection was the direct result of "recent and probably also future technological advances".

In their answers about the changing importance of data protection, overall, our respondents conveyed a rather positive outlook regarding their own sensitivity and awareness towards data protection issues. Most participants, in fact defined themselves as moderately (22%), very (49%) or even extremely aware (22%) of the issue (see figure 4).

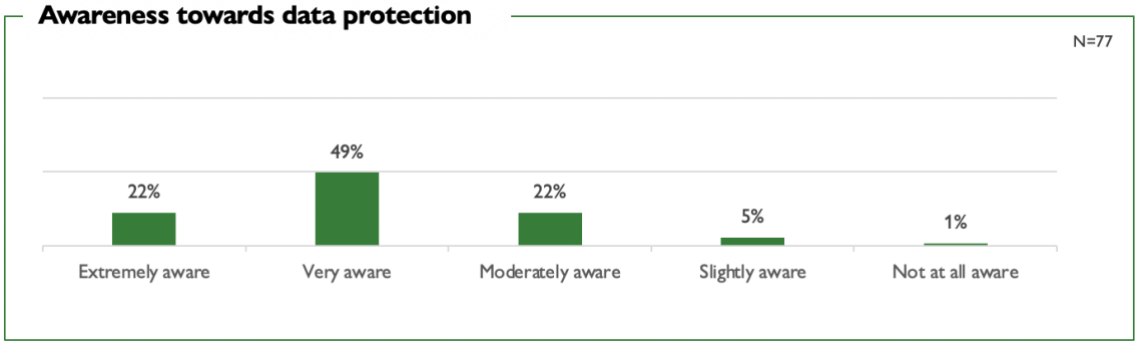


Figure 4: Awareness towards data protection among survey participants

The introduction of the new **regulatory frameworks was of course seen as a driving force** in the shift towards a heightened importance of data protection within law firms. Some respondents for instance mentioned that "the partners were very scared" and that "data protection law forces us to adopt internal policies […] for better protection". Other respondents highlighted the fact that they needed to "live up to rules and regulations" or that they had to "execute data protections measures precisely". Further it was mentioned that "client requirements" caused the topic to be high on the agenda. One respondent for instance explained that:

*"For a good relationship of trust between the client and the law firm, it is essential that the client can trust [the law firm] to handle his or her data with care. The issue of data protection is therefore a high priority in day-to-day work."*

In the open-ended comments participants discussed data protection not only by appealing to the need to protect their clients' confidentiality in rapidly changing digital environments, but also by reflecting on how their firm and the legal sector as a whole was increasingly exposed to data breaches and cyber-attacks. During our survey, we were surprised to notice that 23% of participants admitted that their law firm had been victim of a cyber-attack. Another surprising figure was the fact that out of the 23% who had admitted that their firm had been victim of a cyber-attack only 1% also admitted to a data leak. Whilst we understand that cyber-attacks come in many shapes and forms and not necessarily lead to data leaks, we found the figure surprising and wondered whether it actually reflected the reality on the ground or rather a lack of understanding of the implications of cyber-attacks or a general anxiety towards revealing data leaks. Unfortunately, we do not have an answer to this question.

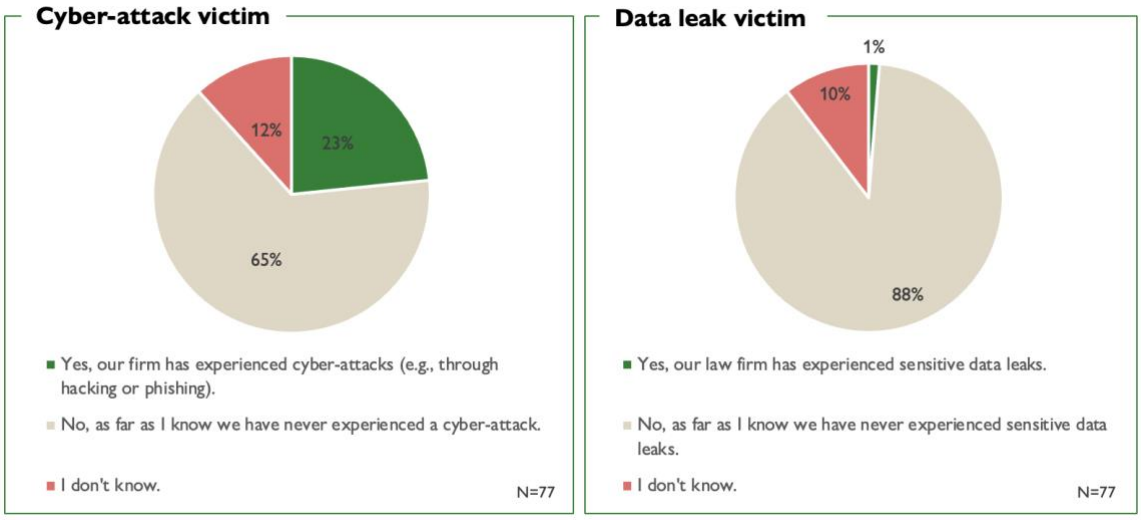


Figure 5: Previous experience of cyber-attacks or data leaks among represented law firms

Another interesting finding of the survey was that amongst law practitioners we are seeing moderate to extreme levels of worry when it comes to reflecting on cyber-attacks and data leaks. Of our sample only 12% indicated that they were slightly or not worried about the issues, whilst 58% of the sample indicated that they were "moderately worried", 27% as "very worried", and 3% "extremely worried" (see figure 6). Based on the participants' comments, we believe that this sense of worry stems from the understanding that the consequences of data breaches and cyber-attacks for law firms can be great and lead to both reputational and financial damages. One participant for instance responded: "[a] leak in data could lead to a massive reputation risk [and a] cyber-attack could force the firm to shut down the services for some time - which would be very costly".

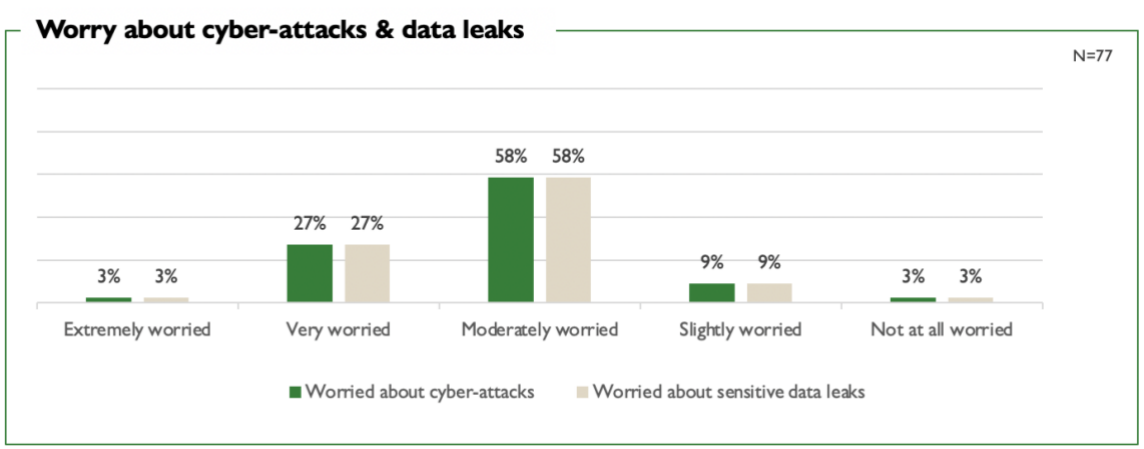


Figure 6: Worry about cyber-attacks and data leaks among survey participants

Further the survey revealed that the sense of worry and urgency towards data protection is slowly but steadily transforming the day-to-day work life of practitioners, who are seeing the **implementation of good data protection practices in their firms.** In this regard different respondents have listed several of these practices. It was mentioned that "relevant systems are in place and updated from time to time", that "regular awareness trainings are conducted", "passwords must meet certain requirements", that "home office [would] only be possible in a very limited way", a "strong frontend" or a "state of the art antivirus software" would be in place, trainings on how to handle or recognize "phishing e-mails" have been conducted, development of "certain tools to mitigate the risk of data leaks and restrict the access to information" or "work[ing] exclusively using a very secure cloud" and with "certified" or "encrypted" emails. Hence within firms we are seeing many important steps towards ensuring data protection and security.

## 3.2 Data Protection: Beliefs, Attitudes and Room for Improvement

Although the surveyed law firms are taking many important steps towards the promotion of good data protection practices and strategies, our survey revealed that law practitioners believed **that there was much room for improvement.** In the open-ended questions, respondents were asked to give a personal assessment of the effectiveness of current data protection practices in their law firm. We were surprised to notice how conflicting responses were, with only few participants being confident and others more cautious and negative. In fact, whilst few of our respondents indicated that data protection within their law firm was "very effective", on a "professional standard" or "top level", many others would be more cautious calling it to be "rather effective", "sufficient" or "quite safe" or openly negative. One law practitioner for instance responded that within his firm data protection seemed to be implemented by a "pragmatic approach on a rather low level" and "the choice of tools and process are not focused on compliance". Others admitted to the following:

> *"There is certainly room for improvement. We are currently doing bits and pieces - not bad, to begin with, but not enough. We lack a proper strategy."*

*"Unfortunately, much less effective than what we advise and recommend to clients."*

*"I think it could be much better. For instance, everybody has access to every file on the cloud, even if we don't need it at all."*

Respondents seemed to be also ambivalent of specific data protection practices employed by firms such as the practice of **outsourcing data protection** to external IT departments or cloud providers. For different participants outsourcing data protection was seen as extremely positive and as proof of the effectiveness of data protection practices in their firm. One respondent for instance mentioned: "We are working with a reliable IT-partner which complies with the applicable laws." Whilst another mentioned: "As we have a cloud provider we trust that he takes care of the data protection practice; we are regularly informed about his activities". Not all respondents shared the enthusiasm for outsourced solutions. Some feared "high-end technological solutions", because these were often complex solutions which escaped their understanding and control. In this regard one participant stated: "Data security falls mostly with fancy solutions and a dependency on third party support". Others from small firms believed these solutions were too expensive.

Of course, the ambivalence in responses could be understood as the reflection of the fact that respondents worked in very different firms in terms of size and business model. Yet what we found interesting is that a similar degree of ambivalence emerged also when respondents answered to the quantitative questions about other key topics such as (1) knowledge of data protection regulations, (2) awareness of security measures, (3) impact of Covid-19:

1. Knowledge of data protection regulations

   One interesting figure in this regard was represented by the fact that the same respondents that defined themselves as moderately (22%), very (49%) or even extremely aware (22%) of the importance of data protection (see figure 4 above) also mentioned that their knowledge of data protection regulations at both national and international levels was far from excellent (see figure 8). The surveyed practitioners felt more confident about their knowledge of data protection at national level, with 26 % of respondents' rating their level of knowledge as excellent; 34% as good; 27% as fair, 9% as poor and 4% as very poor. At international level however these percentages decreased to 17% excellent, 25% good, 24% fair, 27% poor and 6% very poor. This finding is surprising especially if we consider the fact that the overwhelming majority of the surveyed law firms (83%) also revealed that they would serve international clients.

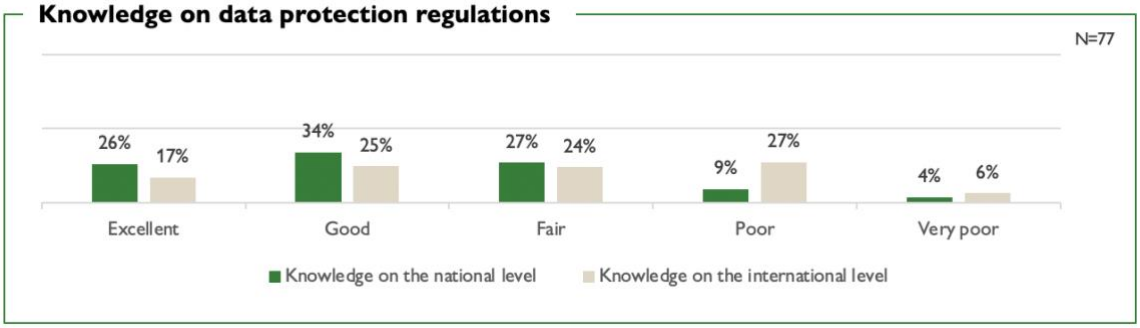


Figure 7: Knowledge on data protection regulations among survey participants

## 2. Awareness of security measures

Another interesting figure that talks directly towards a lack of confidence, can be found in the fact that while respondents seemed to be aware of the fact that heightened security audits in law firms could prevent cyber-attacks and data leaks, they seemed to have only a satisfactory grasp of what was going on in their firm. In fact, just over half (56%) of the respondents indicated that their firm went through security audits, 25% indicated that to their knowledge their firm did not go through security measures and 19% indicated that they did not know. (see figure 9)

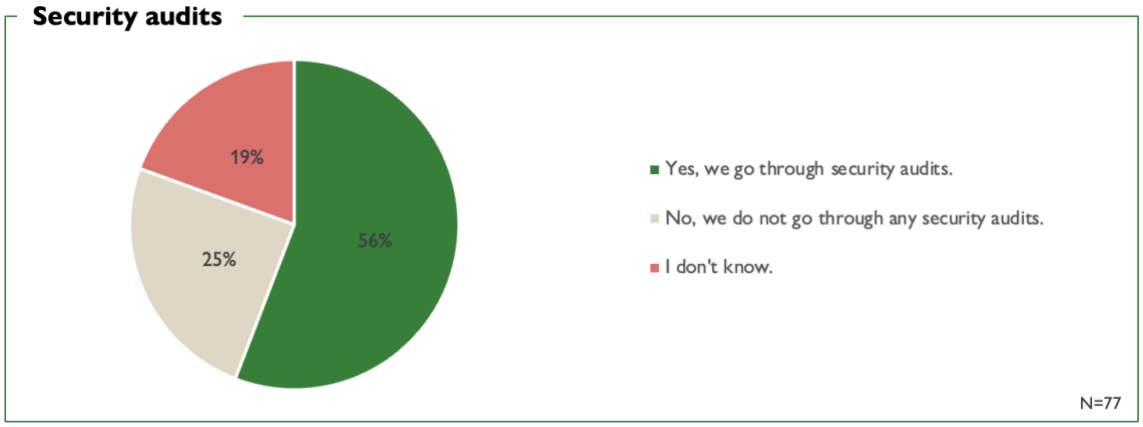


Figure 8: Conduction of security audits among represented law firms

## 3. Impact of Covid-19

Ambivalence was also present in responses that related to the impact that the Covid-19 pandemic and the extension of home office had on respondent's perception of data protection compliance. While only low rates apply to both extremes "very much" (8%) or "not at all" (12%) and even undecided has been quoted only moderately (10%), the vast majorities claims that Covid-19 has either "somewhat" (31%) or "not really" (39%) affected their compliance towards data protection. Yet 39% would admit that their compliance might have been "very much" or "somewhat" affected, which should be considered by law firms that chose to support home office also for the future. Therefore, finding ways to heighten compliance even when working from home, should in this case become a major goal. (see figure 10)

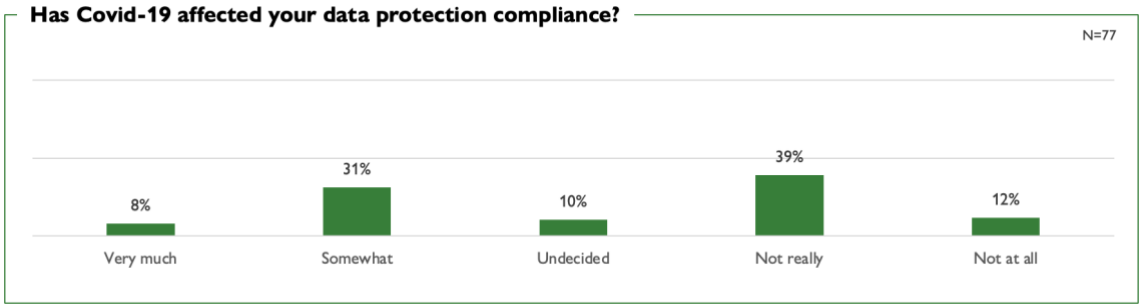


Figure 9: Covid-19 effects on data protection compliance

## 3.3 The Key Challenges to Data Protection in Swiss Law Firms

The ambivalence that emerged clearly from the responses above is not surprising. In fact, it should be seen as a reflection of the fact that - when implementing data protection strategies - law practitioners are confronted with many different beliefs, practical concerns, and barriers which are currently impacting on the implementation of appropriate solutions for data protection as well as on the law practitioners' level of confidence. Overall, our respondents identified **five different challenges** when it comes to abiding to data protection regulations or implementing good practices for data security:

1. Operationality

   Implementing good **data security and protection measures** is seen as **affecting operationality**. Different respondents argued that data protection "makes business sometimes complicated". For instance, one participant mentioned that even though "data protection is indeed important, data has to be available internally so that [they] can work and provide [their] service". Data protection is thus often seen as working against the "need (including clients' expectations) for efficiency, speed, ease of communication". For instance, one participant explained: "In a private enterprise such as a business law firm, we must find a workable middle ground […] between limiting access […] on the one hand, and staying flexible and operational, on the other hand." The understanding that data protection hinders operability is also influencing the rise of negative attitudes towards it. One respondent, for instance saw data protection as a significant economic disadvantage of the EU and Switzerland compared to the U.S. and China. Additionally, legislation has been seen as a source of frustration as it has "derailed onto a formalistic-technical path that created cost, delay and obstacles way out of proportion with, and shifting focus away from, actual reasonable concerns and risks. [It] has become an ideology". Formalistic requirements are seen as a useless burden: "Data security is one thing; formalistic requirements are another. Most of what is considered data protection falls into the latter category. This results in meaningless consumption of (ultimately: the clients') resources. Most, if not all, **clients prefer easy communication and exchange** even considering regular risks and uncertainties". Another respondent added: "Data security is in permanent conflict with user friendliness."

2. Complexity of Data Protection and Lack of Knowledge

Data protection and security are often perceived to be a complex issue which requires: "individual knowledge about how IT works". In this regard one respondent outlined that: "Data security is a wide area and is developing as fast as the technology itself. So it's hard to be up to date on data security." It appears to be a "**technical race in a changing environment to which the human factor has to keep up**". Because data protection and security seem to be pertaining to a 'specialized field of knowledge', there is a general feeling that this knowledge is not easily accessible to all employees, and data training workshops seem not to have yet solved this issue.

3. Lack of Resources and Outsourced Solutions

Data Protection is too resource intensive and time consuming. For this reason, more and more firms rely on outsourced technical solutions to make sure that they meet the data security standards and that they abide to the changing data protection regulations. While outsourced solutions can be key to improve the effectiveness of data protection practices, they can be costly. As shown above, **smaller firms seem to be the most affected** because on the one hand implementing data protection is seen to be "too time-consuming" on the other hand outsourcing data security to experts would be too costly.

4. Role of Clients

Participants also felt that data protection is not only the law firm's job but must also be understood and acted upon by their clients who are transmitting data to them via sometimes unsecure means of communication. One of the main concerns highlighted by the survey is that law practitioners did not know how to address the fact that **many of their clients used weak means of communication** or seemed to struggle in implementing the appropriate data security measures. Another problem was the variety of practices and means of communication that were used by different clients which as one responded explained: "hindered the law practitioners' ability to establish a proper, coherent practice."

5. Organizational Cultures

Respondents pointed out that several hindering mindsets prevail in law firms that prevent them from implementing the appropriate data protection and security measures. For instance, some respondents indicated that they thought that their law firms tend to be overly "confident" regarding their data protection or even "ignorant" of the topic. One respondent also even mentioned that the "law firm's politics" was standing in the way.

# 4 Strategies and Solutions for Data Protection in the Legal Sector

Whilst some of the challenges that have been described by our respondents can be difficult to address, (e.g. organizational cultures) our respondents revealed that the most effective strategy to really achieve change is to **combine behavioural change and IT solutions**. In fact, what we realized is that amongst our respondents those who were confident in the data protection strategies of their firm also believed that their firm had developed a "culture of handling sensitive and confidential data". Indeed, one respondent stressed: "we can rely on the knowledge/experience of our employees, who have internalised that information to third parties must be handled with caution." Their responses focused on the importance of combining IT solutions with behavioural change and seemed to be convinced about the effectiveness of this strategy. One respondent for instance mentioned:

> *"As I'm not only a lawyer but also an IT nerd and data protection enthusiast, the topic itself as well as appropriate practices are high on the agenda. With IT and behaviour, we ensure a high level of protection."*

Two dimensions that are key in enabling behavioural change and successful legal IT solutions are: (1) **Data training** and (2) **File sharing and Technological Solutions**. Hence, we decided to 'zoom-into' these two dimensions to understand their state of the art within Swiss Law firms and how they can be improved.

## 4.1 Data Protection Training and Literacy: How can we Improve?

Whilst it is true that data protection and security can be perceived as a specialized field of knowledge and this can be dauting for many employees in law firms, it is also true that some of the key challenges of data protection implementation can be solved with adequate levels of training and literacy. As one respondent explained:

> *"Data protection is not only about up to date IT [it is also] mainly an educational issue. To protect data in an effective way every person in the company: - must know that we treat sensitive data - must know how to deal with different classes of data - must know how data thieves work (spoofing, phishing, social engineering) to recognize potential attacks - must know how to act in case of a potential data breach."*

Despite training can and should be crucial in achieving behavioural change the findings of our survey suggest a **lack of incorporation as well as further scope of improvement of data training** sessions within Swiss law firms. Indeed, when asked whether they received any training on data protection and corresponding regulations, the participant responses were quite divided. For instance, almost half of the participants responded that they received formal training while

the other **half responded that they did not receive any kind of formal training.** For those who received formal training, these trainings were either received within the law firm (27%) or through a program external to the firm (26%). Amongst those who did not receive any kind of formal training, a significant number of participants (30%) taught themselves about data protection and regulations through readings, videos, or online courses. **17% of the participants mentioned that they did not receive any form of data training**, either formally or informally (i.e., self-taught) (see figure 11, left)

Given these numbers it is not surprising that participants mentioned that they would have appreciated greater quality and frequency of the data training sessions. In fact, **more than 50% of the participants indicated that there is still room for improvement** either in terms of the regularity of trainings or quality of trainings (see figure 11, right).

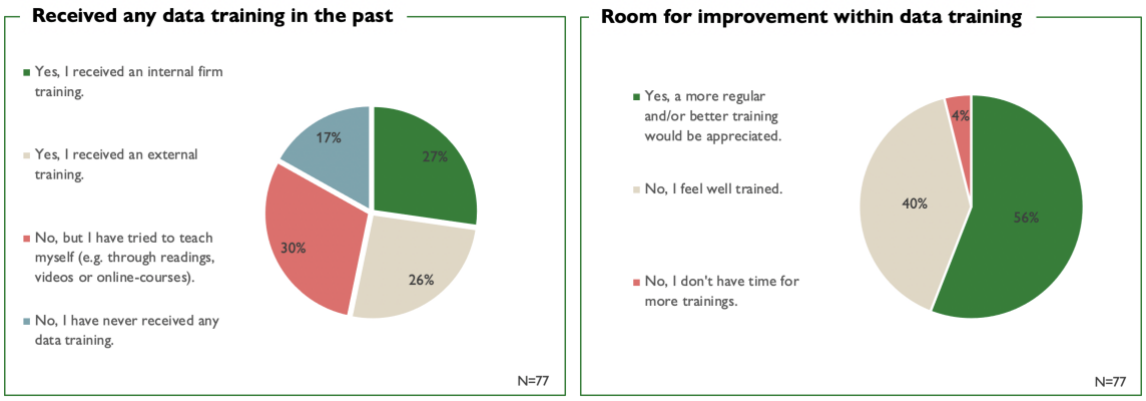


Figure 10: General data training experiences of the participants

Among those who did receive formal data training (N=41, 53%), the participants' answers on the **arrangement of their data training suggested specific factors capable of improvement**. Whilst the survey revealed that data training happened quite regularly - with 37% of the participants who declared that they received their last training within the past three months (see figure 12, left) - one issue that emerged is that training sessions seem not to be mandatory for all law firm employees. In fact, **just over half (54%) of respondents indicated that their firm made these trainings mandatory** (see figure 12, right).

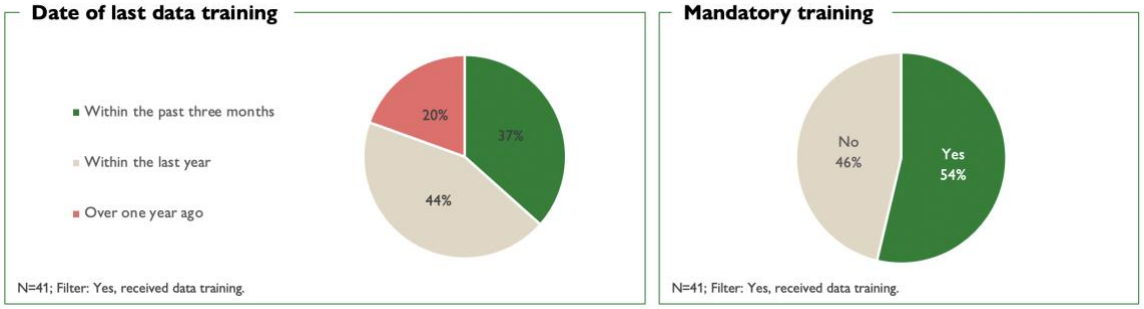


Figure 11: Date of last data training and obligation to participate in data training

The open-ended questions revealed that the respondents felt that training were often **user-unfriendly and included too much information**. For instance, one participant suggested:

*"Any training on data protection should be easy to understand and show the user how he/she can easily implement actions to better protect data. Very often, trainings are overloaded, and people switch off because they think they'll never be able to do all that..."*

A **lack of case studies and real examples for better understanding**, was listed as a problem of content in contemporary trainings. For instance, one of the participants suggested that sharing of experiences and showing examples on cybersecurity attacks like, "phishing attacks or…ransomware attacks" could contribute towards more effective data training sessions. Similarly, another responded believed that "[t]raining should provide concrete answers, not just mention the risks of existing infrastructure". One of the participants illustrated their concern with examples:

*"Many trainings train only good behaviour but do not explain the reason why .. a good training should always tell a story with the reason why behind the explaining point. E.g. telling a story of a case where social engineering helped to easy find the password or showing brute force tools how quick a weak password can be breached or why data classification is that important E.g. user did not realise that stigmatising information was in file or how phishing works ..."*

Another aspect that emerged in our survey was the fact that the **issue of 'file sharing'** – which as we will see below is essential when it comes to the implementation of data protection and data security measures - seems not to be at the top of the agenda in current data training sessions based on our participants experiences. For instance, as shown in figure 13 when specifically asked, 41% participants replied that file sharing practices (e.g. which tools may be employed) are not part of their data training, while 10% of the participants were either not sure or could not remember.

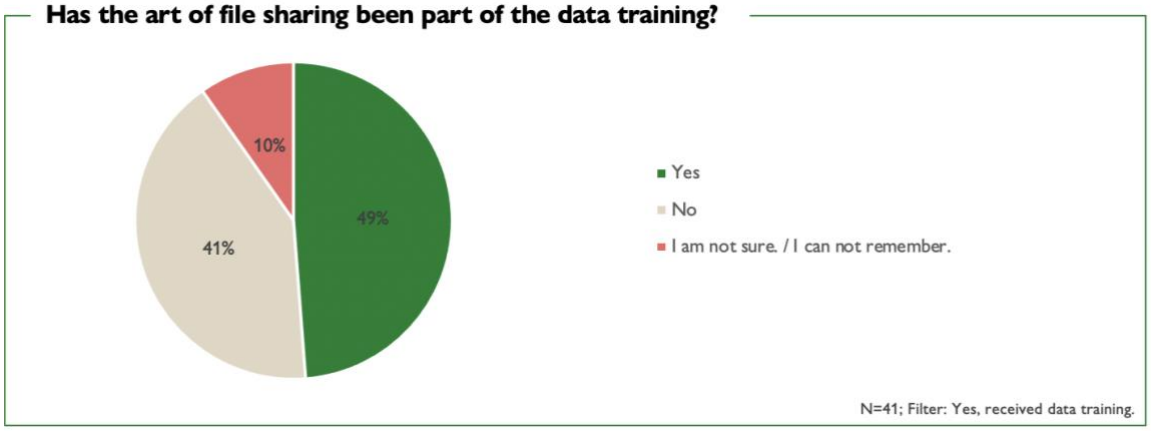


Figure 12: Inclusion of file sharing practices in data training

Perhaps one of our most interesting findings was that respondents indicated that **data trainings did not lead to excellent confidence levels** when it came to data protection compliance. Only a limited number (10%) of participants believed that the data training they had received led them to excellent levels of data compliance, others indicated their level of confidence was good (51%) fair (34%) and poor (5%). (see figure 14)

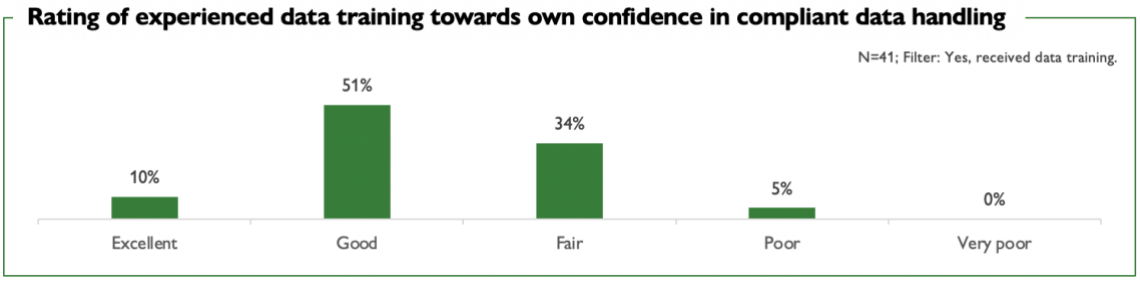


Figure 13: Rating of experienced data training towards own confidence in compliant data handling

The responses of our survey thus led us to the conclusion that current data protection training sessions within law firms have many margins for improvement. The participants also made suggestions regarding the support that the Swiss Bar Association could provide to improve the effectiveness of the data training programs. For example, provision of "guidelines on best practices/ approved solutions" or provision of industry-based solutions for medium and small offices. In addition, we believe that measuring the confidence levels of employees after they received training might be important for law firms to assess whether and how progress is being made towards a change of culture. Indeed, one of the participants from the survey suggested "on-the-job tests" to identify whether the training sessions are aiding good data protection practices. The improvement of data training provisions within law firms and the measurement of their impact, we believe, is of central importance in order to ensure greater data protection literacy and aid behavioural change.

## 4.2 File Sharing, Vulnerabilities and Legal Technology Solutions

File sharing is perhaps the most complex of digital practices when it comes to data protection and data security. Transferring files via electronic communication media has become a substantial part of everyday working routines for law practitioners. Not only must files containing sensitive data be exchanged internally within firms, but also with external stakeholders as as authorities or clients. In this context there is a need for 'good practices' and legal technology solutions that enable secure file transmitting with the highest standards. Law firms that fall behind will likely see a loss of business as client expectations rise and attackers become bolder and more persistent in their efforts targeting law firms. The need for adequate **legal technology solutions** is thus becoming an urgent matter in Switzerland. The Future Ready Lawyer Report (Wolters Kluwer, 2020) found evidence, that while an increasing importance of legal technology is a major concern for 76% of lawyers, only 28% say that their organization is very well prepared for it.

In our survey our aim was to shed light on the state of art of file sharing within Swiss law firms, its areas of weaknesses and improvements. A great majority of our respondents admitted to **sharing files on a daily basis (73%)** and only a limited number admitted to sharing them few times per week (23%). Nearly all participants would **regularly share files with clients (89,6%)** and colleagues within the same office location (88,3%). But also, half of the respondents (58,4%) shared files with official authorities and institutions (e.g., courts) regularly. Also, nearly half of our respondents shared files with colleagues of other office locations (44,2%). While these four groups cover the usual recipients with whom files are shared or from whom files are received, files may occasionally also be shared with the public, associations, university, opponent lawyers

or third parties (e.g., trustees). Another important figure that emerged through our survey is that **72% of all respondents stated to be sharing files across Swiss borders**, with either clients located worldwide (47%) or in Europe (25%). (see figure 15)

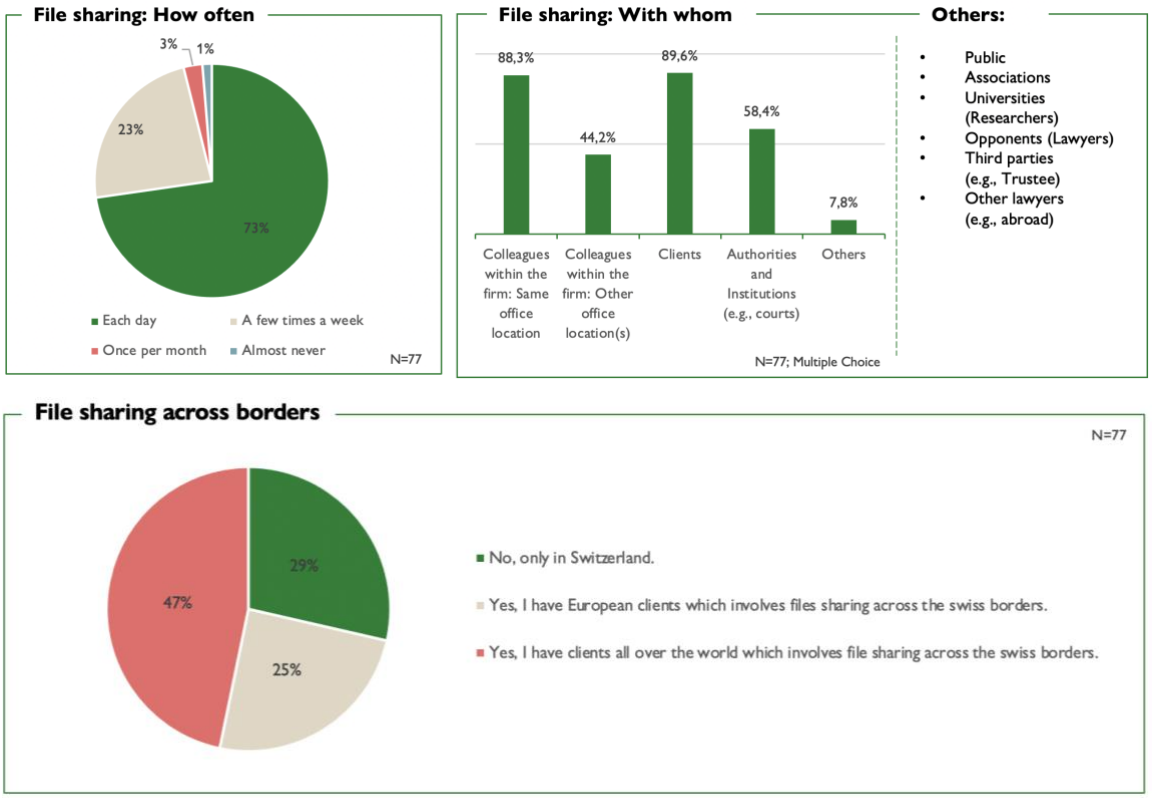


Figure 14: File sharing: Prevalence, Recipients or Senders and Internationality of file sharing activities

Our survey also wanted to highlight which technological solutions the surveyed law practitioners use when it comes to file sharing and whether these legal technology solutions were safe. One of the most interesting findings for us was that an astonishing **90,9% of all respondents indicated to use emails as a main channel for file sharing**. After email the use of internal or external sharing cloud systems was nearly equally popular and approximately used by half of the respondents (55,8%: internal; 49,4%: external). The type of outsourced services that participants used were "Google Drive", "Dropbox, "Microsoft One Drive", "MS Teams" or "WeTransfer", but they also mentioned less popular services as for example "Arcano", "Tresorit" or "Swisstransfer".

Few respondents did also state to use other means than email, internal or external cloud systems. Thus, respondents either referred to especially secured mail by encryption (e.g. SeppMail), traditional post shipments, data carriers as CD or USB or indicated to be using the system as provided and required by the client. (see figure 16)

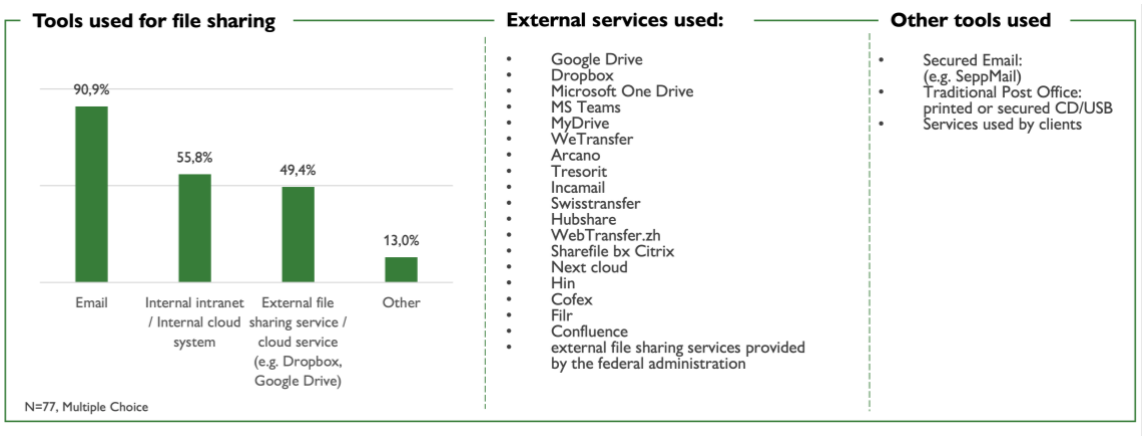


Figure 15: Tools used for file sharing

Survey participants have also been asked whether they would use specific tools when transferring sensitive data. Alarmingly, **only just over half (56%) admitted being using specific tools in the case of sensitive data transfers**. Considering, that almost all respondent indicated to be using "Email" to transfer files this could point to a significant security risk. However, interestingly those who indicated to use popular clouds (e.g. Google Drive), said also that they would not use them to share sensitive data. Instead, they would use more secure tools with additional encryption, multi-factor authentication (MFA, 2FA) or restricted user rights. (see figure 17)

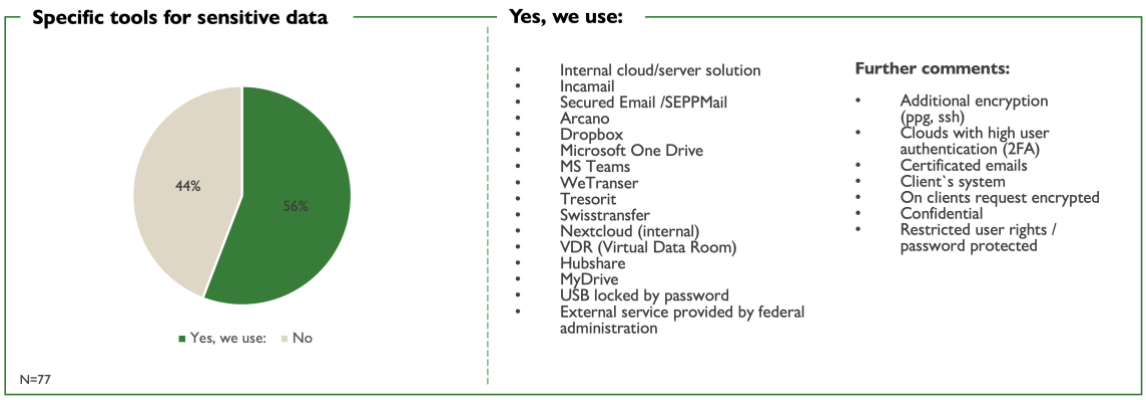


Figure 16: Specific tools used for file sharing including sensitive data

Despite different respondents admitted using more secure tools when it came to sharing sensitive data, overall, our survey revealed that there was a **lack of awareness of the data protection risks of file-sharing** from law practitioners. In fact, 65% of respondents highlighted that they had no concerns in regard to the use of file sharing tools, and a great majority of participants rated themselves as being very confident (36%) or moderately confident (45%) with the tools they were using. (see figure 18)

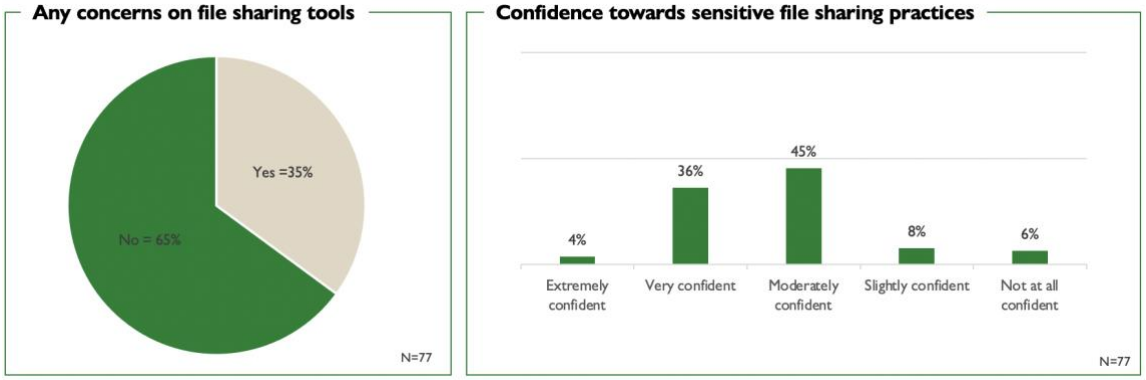


Figure 17: Concerns on file sharing tools and confidence towards sensitive file sharing practices

A great majority of respondents seemed to share a lack of awareness about the risks of file sharing. Yet some respondents shared their concerns in relation to malpractices in the open-ended questions. For instance, different participants indicated that they **did not feel comfortable with the fact that emails are widely used to transfer files**. Some of the comments we received can be found here below:

*"Too often, files are sent via normal e-mail (i.e. no secure transmission)"*

*"99% of our e-mail and sharing traffic is not secure at all."*

*"Often we use normal e-mail which is not a secure way of sharing data."*

*"As Emails aren't always as protected as it may seem it's vital to check to not send any sensitive data unencrypted."*

*"I am not sure it is really safe. It seems to be a simple mailbox as everyone has. I think lawyer should use more secured tools."*

**Client malpractices** were listed as a problem when it came to file sharing:

*"Additional security measures should be taken to communicate certain files and information (like encryption) but recipient[s] often lack the technological tool to allow for encrypted communication."*

*"I am not a fan of sharing files via e-mail, because I know, that's not really safe. So I only use it, when the clients want it that way and clarify the risk of data leaks."*

*"Certain divisions in our firm use, based on client requests, dropbox or other popular file-sharing tools."*

*"Clients not only consent to unsecure e-mail correspondence, they ask us to do so. We offer a secure file sharing platform (PrivaShere), which is used by clients 2 - 3 times per year."*

When it comes to file sharing, a **crucial solution** for law firms could be to **invest in appropriate legal technology**. In Switzerland we are seeing many important steps forward in legal tech innovation especially when it comes to file sharing. For instance, some Swiss authorities have even built their own transfer systems, as for instance the cantonal administration of Zurich, which is using "WebTransfer ZH", which is a service that must be used by lawyers when sharing files with the cantonal administration. Also, the Swiss legislative authorities are currently undergoing a big digital transformation called "Justitia 4.0": *"The Justitia 4.0 project is meant to drive the digital transformation of the Swiss justice system regarding criminal, civil and administrative court proceedings. The aim is to facilitate access to justice and speed up proceedings. By 2026, electronic legal transactions and electronic file inspection are to take place between all parties involved in judicial proceedings (courts, public prosecutors' offices, bar) at the cantonal and federal level via the central platform "Justitia.Swiss". Paper files will be replaced by electronic files and the working environment and infrastructure in the justice system will be optimized."* (Justitia40.ch, translated from German). In addition to this we are also seeing the rise of Swiss private businesses developing file sharing solutions (e.g., Arcano, Tresorit or SwissTranfser,) some of which are Privacy by Design. The incorporation of Privacy by Design principles is an indispensable requirement for data protection especially, within the law firms. Instead of implementing "reactive" and "remedial" solutions to data breaches that already happened within the system or organization, this principle can help law firms in taking "proactive" and "preventative" measures "before-the-fact" to avoid potential data losses (Cavoukian, 2009).

Unfortunately, what we discovered through our survey was that the level of awareness or **familiarity with legal technology solutions** for file sharing, and especially **Privacy by Design/Default solutions**, was **extremely low.** As shown in figure 19 (left), while 55% of the participants were aware of Privacy by Design/Default principles, 45% participants responded that they have never heard of the term. Only a small share of 19% was able to think of any PbD settings currently in place and name corresponding examples. On the one hand, this can be explained through the vast number of participants that have never heard of PbD, but on the other hand, the only few given examples also reveal an actual lack of Pbd settings or implementation of technologies supporting PbD

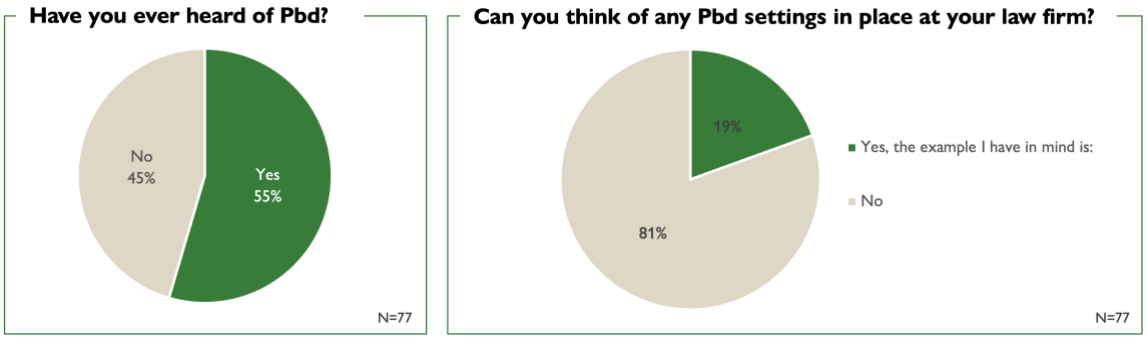


Figure 18: Participant knowledge on Privacy by Design and current employment in law firm

Still, in open ended questions some participants highlighted that for them Privacy by Design was important for "enhancing data protection and avoiding mass data breaches" and "Privacy by Design can in many cases compensate unmindful acting of users". Greater awareness of the legal technology solutions available as well as appreciation of the benefits of privacy by

design we believe could be crucial in the implementation of good data protection and security practices especially in those firms where behavioural change is not happening.

Finally, the survey not only showed that a greater usage of legal technology solutions that support Privacy by Design could strengthen data protection by Swiss law firms, but also revealed various **important factors to be kept in mind by legal technology providers**, who strive to support data protection within Swiss law firms. It became obvious that smaller law firms will easily be left behind in their endeavours for data protection as they do not have the resources in terms of time and money to build sufficient knowledge on data protection or to buy external support. Therefore, legal technology solutions become an important aid especially for smaller law firms. However, they must be affordable, easy to understand and implement as well as transparent in their data protection strategy. Equally important remains the user-friendliness which is defined by the operationality of the system, both for the law firm and law firms' clients. Client requirements have been named as one of the most urgent external factors influencing the law firm's data protection. Therefore, motivating or convincing the client to use secure file sharing tools comes down to the ease of use incorporated into legal technology solutions.

# 5 Conclusions

The rapid digitalization of day-to-day working life amongst Swiss law practitioners and new data protection regulations have placed the issue of 'data protection' at the top of the agenda for law firms in Switzerland. Whilst data protection and client's privacy have always been important for the legal sector, and as our respondents have shown have been an "[e]ssential part of [their] professional activity" or even the "foundation of lawyer's work", the survey revealed that law practitioners are changing their attitude towards data protection. Today data protection is seen as being not only essential to guarantee the client's right to privacy in increasingly complex digital environments but also fundamental for protecting the law firm against cyber-attacks and data leaks.

The aim of this survey was to shed light and give voice to the beliefs, practices and challenges that law practitioners face in their everyday work life when it comes to data protection, and what solutions they are envisaging for their firms and the legal sector in general. While some research can be found that discusses issues of data protection in regard to Swiss companies in general (PwC, 2018; Patklom, 2018), so far, we lacked a critical and qualitative understanding of the problems that emerge in everyday practice for law firms, of the ways in which legal practitioners understand data protection, or what they think about the technologies they use.

As shown in this report, our respondents conveyed a rather positive outlook regarding their sensitivity and awareness towards data protection issues. Law practitioners understand clearly that data breaches, leaks or misuse can have a major impact on the reputation of the firm as well as its finances. The sense of worry and urgency towards data protection is slowly but steadily transforming the day-to-day work life of practitioners, who are seeing the **implementation of good data protection practices in their firms.** Although firms are taking many important steps towards the promotion of good data protection practices and strategies, our survey revealed that law practitioners believed **that there was much room for improvement.** However, one fundamental aspect that emerged through our survey was an **ambivalence of attitudes and first-hand experiences** of data protection. In fact, we received many contradictory responses when it came to assessing the effectiveness of the data protection in their firms. This ambivalence was evident also with reference to the ways in which practitioners measured their knowledge of data regulations, their awareness of security checks within their firm or the impact of Covid-19.

We believe that the ambivalence that emerged clearly from the responses was not surprising. In fact, it should be seen as a reflection of the fact that - when implementing data protection strategies - law practitioners are confronted with many different challenges. Our survey highlighted **five different yet interconnected challenges** that make the pursue of greater data protection and security difficult. A fundamental issue that emerged in our responses was the *problem of operability* and the fact that data protection makes business more complicated and less efficient. Another fundamental problem was the perception that data protection and security were ever-changing, that respondents were involved in 'technical race in a changing environment to which the human factor has to keep up' and in a *field of knowledge that was too complex and too specific*. Our survey also revealed that data protection is seen to be *too resource-intensive* and that outsourcing data security to experts is too costly especially for smaller firms. In addition to these

problems our respondents also listed the *malpractices of clients* as well as the *organizational cultures* of firms as barriers to ensuring greater data protection and security.

Whilst some of the challenges that have been described by our respondents can be difficult to address, our respondents revealed that the most effective strategy to really achieve change seems to be the strategy of combining **behavioural change and IT solutions**. In fact, what we realized is that amongst our respondents those who were confident in the data protection strategies of their firm also believed that their firm had developed a "culture of handling sensitive and confidential data". During our survey we thus decided to "zoom-in" and analyse: (1) How legal practitioners understand and experience **data training** and (2) how legal practitioners share data through the practice of **file sharing** and whether more adequate (Privacy by Design) legal technology solutions are needed.

What we realized is that in both areas there is much margin for improvement. In fact, on the one hand our survey revealed that law practitioners believed that data training experiences did not give an excellent level of confidence in individual data compliance strategies. They also suggested that in many cases the trainings lacked hands-on examples, were too overloaded or even not mandatory. With reference to file-sharing practices our survey revealed that **only just over half (56%) admitted being using specific privacy preserving tools in the case of sensitive data transfers** and that overall, the respondents showed a **lack of awareness of the data protection risks of file-sharing.** Greater attention to the ways in which data training is organized within Swiss law firms, as well as better investment in Privacy by Design solutions, we believe would be an important starting point to overcome some of the issues and challenges that Swiss law firms face in the implementation of good practices of data protection and security.

There are of course **a number of limitations** that come with our study which can be addressed in future research. In the first place, this study was mostly concerned with problematizing the issue and giving voice to the experiences and attitudes of law practitioners. It is for this reason that we have chosen to rely on both quantitative questions and qualitative open-ended questions and on a small sample (50-100 participants). Because of its **inherently qualitative approach**, this study does not want to and cannot be considered as statistically significant. Another fundamental limitation of our study is the actual sample. As mentioned in the introduction, the recruitment phase was challenging to say the least as data protection is perceived by many as the 'Achille's heel' of Swiss law firms, and we believe that it is for this reason that especially junior staff/non legal staff and others did not feel that they could talk openly about these problems. This resulted in the fact that our sample was constituted mostly by senior law practitioners 64% who identified themselves as partners and 78 % who identified themselves as being part of the decision-making process. A third limitation of our survey is that it was not able to test the efficiency of specific legal technology solutions, such as Privacy by Design solutions. What we aimed to do with this project is to offer those developing legal technology solutions a critical and in-depth understanding of the problems that emerge in everyday practice.

# References

Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles—Implementation and Mapping of Fair Information Practices*. Information & Privacy Commissioner. https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

Cepero, R. (2020, July 17). *How Law Firms Can Protect Their Client's Data*. Bleuwire. https://bleuwire.com/how-law-firms-can-protect-their-clients-data/

CMS Legal (2021, December 01). E-Privacy – European Regulation on Privacy and Electronic Communication. Retrieved from https://cms.law/en/deu/insight/e-privacy(17. June 2022)

Fischer, B. (2020, March 2). What is the Average Cost of a Data Breach? SCA Security Compliance Associates. https://www.scasecurity.com/cost-of-a-data-breach/

Gross, H. (2022, March 4). *Neues Datenschutzgesetz: Was müssen Schweizer Unternehmen beachten.* AXA-ARAG. Retrieved from https://www.axa.ch/de/unternehmenskunden/blog/sicherheit-und-recht/recht-und-justiz/neues-datenschutzgesetz.html (17. June 2022)

Matich, T. (2021, January 19). *2021 Law Firm Data Security Guide: How to Keep Your Law Firm Secure*. Clio. Retrieved from https://www.clio.com/blog/data-security-law-firms/ (17. June 2022)

Nabe, C. (2020). *Impact of COVID-19 on Cybersecurity.* Deloitte. Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (27 June 2022)

Ng, C. (2020, March 29). *Why Law Firms Should Care About Data Security.* Varonis. Retrieved from https://www.varonis.com/blog/why-law-firms-should-care-about-data-security/ (17. June 2022)

Official Website of the Swiss Government (n.d.) *Die Sprache – Fakten und Zahlen*. Retrieved from https://www.eda.admin.ch/aboutswitzerland/de/home/gesellschaft/sprachen/die-sprachen---fakten-und-zahlen.html (17. June 2022)

Patklom, T. (2018). *Herausforderungen bei der Umsetzung des Datenschutzes für ein Schweizer Unternehmen*. Zürich: Schulthess Verlag.

PwC (2018). *Was bringt die Revision des Schweizer Datenschutz-gesetzes mit sich, und wie hängt dies mit der DSGVO und der ePrivacy-Verordnung zusammen.* PwC. https://www.pwc.ch/de/publications/2018/E-DSG_Revision-des-Schweizer-Datenschutzgesetzes.pdf (17. June 2022)

Swiss Global Enterprise (2019). *GDPR – Information Sheet.* Retrieved from https://www.s-ge.com/sites/default/files/static/downloads/european-general-data-protection-regulation-gdpr-s-ge-2019-03.pdf (27. June 2022)

Tillay, M. (2021, February 23). *Why Cybersecurity Has Become a Bigger Problem For Law Firms.* Retrieved from https://www.law.com/international-edition/2021/02/23/why-cybersecurity-has-become-a-bigger-problem-for-law-firms/ (accessed 17 June 2020).

Wolters Kluwer (2017, November 22). *GDPR: How it will impact your law firm and what lawyers need to know.* Wolters Kluwer. Retrieved from https://www.wolterskluwer.com/en-gb/expert-insights/gdpr-will-impact-law-firms-what-lawyers-need-to-know (17. June 2022)

Wolters Kluwer (2020) *The 2020 Wolters Kluwer Future Ready Lawyer Survey: Performance Drivers Report.* Wolters Kluwer. Retrieved from https://know.wolterskluwerlr.com/2020-Future-Ready-Lawyer (17. June 2022)

Wolters Kluwer (2021, February 8). *Optimising document work in law firms, legal departments with legal tech tools.* Wolters Kluwer. Retrieved from https://www.wolterskluwer.com/en-gb/expert-insights/optimising-document-work-in-law-firms-legal-departments-with-legal-tech-tools (17. June 2022)

Wolters Kluwer (2021, January 25). *The future of software for law firms: from mandate acquisition to digital case processing*. Wolters Kluwer. Retrieved from https://www.wolterskluwer.com/en-gb/expert-insights/the-future-of-software-for-law-firms-from-mandate-acquisition-to-digital-case-processing (17. June 2022)

Zhang, E. (2020, August 6). *5 Tips For Protecting Sensitive Data At The Law Firm.* Digital Guardian. Retrieved from https://digitalguardian.com/blog/5-tips-protecting-sensitive-data-law-firm (17. June 2022)

# List of Abbreviations

ABA American Bar Association
DSG Datenschutzgesetz (Data Protection Law)
E-DSG Entwurf des Datenschutzgesetzes (drafted Data Protection Law)
EEA European Economic Area
ePR electronic Privacy Regulation
EU European Union
GDPR General Data Protection Regulation
nDSG neues Datenschutzgesetz (new Data Protection Law)
SAV Schweizerischer Anwaltsverband (Swiss Bar Association)
PbD Privacy by Design / Privacy be Default

# List of Figures

Figure 1: Participant's characterization within law firm 5
Figure 2: Characterization of represented law firms 6
Figure 3: Office structure and client's internationality of represented law firms 6
Figure 4: Awareness towards data protection among survey participants 7
Figure 5: Previous experience of cyber-attacks or data leaks among represented law firms 8
Figure 6: Worry about cyber-attacks and data leaks among survey participants 9
Figure 8: Knowledge on data protection regulations among survey participants 11
Figure 9: Conduction of security audits among represented law firms 11
Figure 10: Covid-19 effects on data protection compliance 12
Figure 11: General data training experiences of the participants 15
Figure 12: Date of last data training and obligation to participate in data training 15
Figure 13: Inclusion of file sharing practices in data training 16
Figure 14: Rating of experienced data training towards own confidence in compliant data handling 17
Figure 15: File sharing: Prevalence, Recipients or Senders and Internationality of file sharing activities 18
Figure 16: Tools used for file sharing 19
Figure 17: Specific tools used for file sharing including sensitive data 19
Figure 18: Concerns on file sharing tools and confidence towards sensitive file sharing practices 20
Figure 19: Participant knowledge on Privacy by Design and current employment in law firm 21