Juristische Zeitschrift für Pharma, Biotech und Medtech
Revue juridique des technologies pharmaceutiques, bio- et médicotechniques
Law journal for pharma, biotech, and medtech

Life Science Recht

www.LSR.recht.ch

4/2023

online+
Ihre Vorteile auf einen Blick: Seite 232

en ligne+
Vos avantages en un coup d'oeil : Page 232

Stämpfli Verlag

The New Data Protection Act: Challenges for Pharmaceutical Companies

Managing Website Data Privacy Notices Under the New Regulations

Marcel Boller
Dr. iur., Attorney at Law, Wenger Vieli AG, Zurich

Luana De Luca
MLaw, LLM, Junior Lawyer, Wenger Vieli AG, Zurich

Keywords: Pharma, Data Privacy

Abstract: In light of Switzerland's revised Data Protection Act, the pharmaceutical industry confronts an increasingly complex regulatory terrain. This legislation, designed to fortify personal data protection and synchronize with European norms, exerts substantial influence over healthcare-related activities. This article delves into the essential clauses of the Act, scrutinizes their ramifications for pharmaceutical enterprises, and offers pragmatic guidance for navigating compliance intricacies.

Table of Contents

I. Introduction

As technological progress accelerates, data has become a cornerstone of the healthcare industry, commanding increased attention and regulation. Pharmaceutical companies, positioned at the nexus of healthcare and innovation, face new legal obligations designed to secure sensitive data. Switzerland's revised Data Protection Act (hereinafter "DSG") serves as a recent milestone in this regulatory journey. Tailored to bolster personal data protection, this legislation amplifies the complexities of compliance for pharmaceutical companies. This paper aims to explore these new challenges, focusing on their implications for data privacy notices on websites of pharmaceutical companies.

II. Art. 19 DSG: Implications for Data Privacy Notices on Websites

Following the entry into effect of the new DSG on 1st September 2023, there has been a significant shift in the Swiss legal landscape. The new Art. 19 DSG entails a significant extension of the duty to provide information.[1] Specifically, the mandatory information

1 Kurt Paerli/Nathalie Flueck, Kommentar zu Art. 19 DSG, in: Datenschutzgesetz (DSG), Stämpflis Handkommentar (SHK), Ed. 2, Bern 2023, p. 237.

requirements for both private individuals and public authorities have been increased and clarified. This means that even if personal data is collected with a low risk of privacy violations, the data subject concerned must be adequately informed. In addition, the information requirements are no longer limited to the collection of sensitive personal data, but now apply to all personal data, unless one of the exceptions under Art. 20 DSG applies.[2] While the transparency obligation under Art. 6 DSG creates a basic level of transparency, the duty of information under Art. 19 DSG builds on this in order to satisfy a more extensive need for information. The data controller must thus not only ensure that the data collection is recognisable as such, but must also provide the data subjects with certain information on the purposes and methods of the processing.[3]

In addition, compliance with the duty to provide information now entails additional costs and risks for companies, as data controllers with inadequate data privacy notices risk a fine of up to CHF 250,000 under Art. 60 DSG and the justifications for data protection violations under Art. 31 DSG are no longer applicable.[4]

In the pharmaceutical sector, the implications of the new Art. 19 DSG should not be underestimated. The revised legislation expands the scope of information requirements for the collection of data. This necessitates that pharmaceutical companies undertake a thorough review of their existing data privacy notices. Failure to adapt to these new mandates not only risks non-compliance, but also exposes the companies to significant legal and reputational risks. Therefore, the implementation of the revised DSG is of paramount importance for risk mitigation and legal compliance in general, including in the pharmaceutical sector.

A. Transparency in Data Collection

According to Art. 19(1) of the DSG, the burden of information falls on the data controllers which are obliged to appropriately inform individuals when collecting personal data.[5] For example, if a pharmaceutical company gathers data about website usage from its customers, it is obligated to notify these customers accordingly. This emphasizes the need for clear communication channels, particularly in the digital realm.

The duty of information applies only to the intended or planned collection of personal data. If the data are accrued accidentally or unintentionally (e. g. through unsolicited email inquiries), the data controller is not obliged to inform the data subject unless the personal data are used for a new or additional purpose.[6]

The guidelines for ensuring the adequacy of the information are detailed in Art. 13 of the Data Protection Ordinance (hereinafter "DSV"). The information must be provided in a clear, transparent and easily accessible manner in order to be comprehensive. The accessibility requirements to be imposed must be assessed on a case-by-case basis, taking into account the risk of privacy violation, the nature of the personal data collected and the scope of the data processing. Therefore, the duty to provide information requires the data controller to provide all necessary information in a way that enables the data subject to access it independently and in a reasonable manner. In practice, most companies use a privacy notice or a privacy policy to fulfil this obligation.[7]

The duty to provide information applies to any (new) collection of personal data. It also applies when personal data that has already been collected is used for a new or additional purpose, or when a new joint controller is involved. This means that subsequent changes (e. g. in the storage of the data or new categories of recipients) do not need to be communicated to the data subject, unless the collected data is used for a purpose other than the one stated. Therefore, and with regard to existing customers or patients, there is no need to proactively inform them of the revised DSG as long as no new data is collected and the purpose of the collection remains in scope. The opposite was partly the case when the EU General Data Protection Regulation (hereinafter "GDPR") came into force. It will now be sufficient to provide the additional data privacy notices on the company's own website.[8]

B. Mandatory Information Requirements

Art. 19(2) DSG outlines a minimum set of information that must be provided to individuals. As a minimum,

2 See Chapter III(B) for more details; David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16 November 2020, p. 36; Kurt Paerli/Nathalie Flueck (fn. 1), p. 236, 243 et seq.

3 Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 19 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version 20. 8. 2023, n. 5, available at: https://onlinekommentar.ch/de/kommentare/dsg19.

4 David Rosenthal (fn. 2), p. 36; Kurt Paerli/Nathalie Flueck (fn. 1), p. 246; Kurt Paerli/Nathalie Flueck (fn. 1), p. 236, p. 243 et seq.

5 Data controller is the individual who decides alone or jointly with others on the purposes and means of the intended data processing (Art. 5(j) DSG); Kurt Paerli/Nathalie Flueck (fn. 1), p. 238; Matthias Glatthaar/Annika Schröder (fn. 3), n. 13.

6 David Rosenthal (fn. 2), p. 37; Kurt Paerli/Nathalie Flueck (fn. 1), p. 238; Matthias Glatthaar/Annika Schröder (fn. 3), n. 16.

7 In principle, it does not matter which medium is used to provide the information and whether the data subject actually accesses the information, Art. 19 DSG only requires that it is made adequately available. Therefore, companies should ensure that their data privacy notices are easily accessible and simple to find on their website with just a few clicks. A common approach is to describe a broad range of data processing in a general privacy notice and to supplement this with multiple product- and service-specific statements; David Rosenthal (fn. 2), p. 39; Kurt Paerli/Nathalie Flueck (fn. 1), p. 241 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 43 et seq., n. 48.

8 David Rosenthal (fn. 2), p. 37; Matthias Glatthaar/Annika Schröder (fn. 3), n. 17, n. 59.

the data subject must be provided with the information necessary to exercise his or her rights and to ensure the transparency of data processing. This general provision is supplemented by the following requirements:

- the identity and contact details of the data controller (Art. 19(2)(a))
- the purpose of the processing (Art. 19(2)(b))
- if applicable, the recipients or at least the categories of recipients to whom personal data are disclosed (Art. 19(2)(c))

In particular, the contact details should include the postal address and telephone number or email address of the data controller. If the data controller is domiciled abroad, the name and contact details of an appointed representative in Switzerland must be provided (Art. 14 DSG).[9]

The purpose of the processing must be described as accurately as possible. However, the more precisely the purpose is defined, the greater the risk for the data controller that the communicated processing purposes will be interpreted restrictively, in accordance to the principle of trust and the ambiguity rule. Therefore, privacy notices may also mention possible future purposes of processing to avoid the need to constantly provide new information.[10]

It is necessary to indicate the recipients of the personal data, as well as joint data controllers and processors. However, it is not mandatory to identify the firm's own employees or departments, nor the individual recipients, but only the category of recipients.[11]

It is important to note that according to the new Art. 19(2) DSG, the information must be provided at the time of collection. This means that the data subject must be informed at the latest when the data is collected. Thus, the information should at least be available on the data controller's website at that time. This differs from the past DSG, where information was considered permissible immediately after data collection. Prior information is only considered sufficient if the link between the information and the collection is obvious to the data subject.[12]

C. Additional Obligations for Indirect Data Collection

In addition to the mandatory information requirements, Art. 19(3) and 19(5) of the DSG lay out specific obligations for scenarios where data is not directly collected from the individual. This is particularly pertinent for companies sourcing data from third parties.

The duty to provide information applies both when the data is collected directly from the data subject and when the personal data is collected from third parties.[13] If the data has not been collected directly from the data subject and the data subject is unaware that the company is processing personal data, active communication is required. In such cases, data subjects must be actively made aware of the data privacy notice, e.g. by providing the URL or a QR code via email, in order to prevent data violations. In addition, information must be provided even if the data are inadvertently or unintentionally collected from third parties, if such personal data is to be used for new or additional purposes anyway.[14]

In cases of indirect data collection, the data subject must be informed of the categories of personal data processed as an additional requirement (Art. 19(3) DSG). If the data subject is not aware of the data processed and has a need for information, it is important that the level of detail is meaningful and sufficiently informative. It is helpful, but not necessary, if the categories can be linked to specific processing purposes. As a preventive measure, it is advisable to specify the categories of data processed even when the data are collected directly from the data subjects but without their active involvement and they may therefore not be aware that data about them are being processed.[15]

Furthermore, the required information does not have to be provided immediately, but only within one month of the receipt of the data (Art. 19(5) DSG). However, the one-month period presupposes that the personal data are not disclosed by the recipient to another party. Otherwise, the information must be provided when the data is disclosed. As this includes disclosures to processors (e.g. cloud services), in most cases the deferral has little practical significance, so the information must be provided immediately.[16]

If direct communication with the data subject is not possible, the data controller must invoke an exception as outlined in Art. 20 of the DSG. Such exceptions may apply when the data subject is already aware of the pertinent information or when data processing is mandated by law. The provision of Art. 19

9 Kurt Paerli/Nathalie Flueck (fn. 1), p. 239; Matthias Glatthaar/Annika Schröder (fn. 3), n. 23 et seq.

10 Short descriptions such as "direct marketing", "product development" or "fraud prevention" are acceptable; David Rosenthal (fn. 2), p. 37; Kurt Paerli/Nathalie Flueck (fn. 1), p. 239.

11 For example, "cloud service", "IT service provider", "logistics company", or even broad categories such as "processor"; David Rosenthal (fn. 2), p. 38; Kurt Paerli/Nathalie Flueck (fn. 1), p. 239; Matthias Glatthaar/Annika Schröder (fn. 3), n. 26 et seq.

12 David Rosenthal (fn. 2), p. 37; Kurt Paerli/Nathalie Flueck (fn. 1), p. 240; Matthias Glatthaar/Annika Schröder (fn. 3), n. 41.

13 Direct acquisition occurs when the data subject voluntarily provides the data to the data controller or when the data controller collects the data through observation or automated means. Indirect acquisition occurs when the controller collects data from public sources, receives data from third parties, or derives new data from existing records; Matthias Glatthaar/Annika Schröder (fn. 3), n. 40.

14 David Rosenthal (fn. 2), p. 39; Kurt Paerli/Nathalie Flueck (fn. 1), p. 237 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 55.

15 Categories could be described as "master data", "health data" or more specific as "name", "email", etc.; Kurt Paerli/Nathalie Flueck (fn. 1), p. 237 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 29 et seq.

16 Matthias Glatthar/Annika Schröder (fn. 3), n. 42.

holds significant implications for pharmaceutical firms, especially when sharing patient information with insurance providers or healthcare services without obtaining the data directly from the data subject and thus without consent.[17]

D. International Data Transfers

With many pharmaceutical companies operating on a global scale, the provisions of Art. 19(4) of the DSG, relating to international data transfers, are especially significant.

In cases where the personal data collected are disclosed[18] abroad and/or the recipients of the data are located abroad, the countries concerned must be identified and disclosed to the data subject. However, it is sufficient to specify the groups of countries and regions involved. This means that designations such as "EU", "all countries in which we operate" or "worldwide" satisfy the requirements of Art. 19 DSG, as these countries can be defined. The term "worldwide" is permissible because it is clear to the data subject that his or her data may be processed in any country in the world.[19]

If the recipient countries include countries without an adequate level of data protection, additional information must be provided. In particular, it must be stated which data protection safeguards pursuant to Art. 16(2) DSG apply to ensure an adequate level of data protection. Alternatively, it must be specified which exceptions under Art. 17 DSG enter into consideration. Here the DSG differs from the GDPR.[20]

E. Conclusion

In summary, the revised DSG signifies a paradigm shift in the realm of data protection, most notably by expanding the duty of disclosure from a narrow focus on sensitive personal data to encompass all forms of personal data. This represents a broadening of responsibilities for data controllers, requiring them to be meticulous in the dissemination of information related to data collection and processing. The new regulations also stipulate more proactive communication in certain scenarios, particularly when data is acquired indirectly and the data subject is therefore unaware of the company processing his or her data. This is of utmost importance for pharmaceutical companies, who often need to exchange sensitive patient data with third-party entities like insurance companies and healthcare providers.[21]

III. Gaps Between Art. 19 DSG and the Provisions of the GDPR

The objective of the DSG is to elevate Swiss data protection standards to align with those of the European Union. However, there are distinct differences between the revised DSG and the GDPR. Some of these variances directly impact the manner in which pharmaceutical companies collect and process personal data online. Although most pharmaceutical companies may fall under the jurisdiction of the GDPR and therefore already comply with most of the provisions of the new DSG, there are some gaps to be aware of.

A. Guidance by the GDPR

In drafting the new Art. 19 DSG, the Swiss legislator was guided by Art. 13 et seq. GDPR, which is not binding in Switzerland but must be taken into account when interpreting the law in order to achieve a level of data protection equivalent to that of the EU. Furthermore, due to its extraterritorial effect, the GDPR may also apply to processing operations and data subjects in Switzerland. The information requirements under Art. 19 DSG are largely the same as those under Art. 13 GDPR, although the GDPR contains a more comprehensive catalogue of information to be provided. Specifically, Art. 13 GDPR requires that the legal basis for the processing, the duration of the processing, the existence of individual rights of access, rectification, erasure, restriction, objection, data portability and revocation of consent, as well as the right to appeal, must be communicated.[22] The DSG, on the other hand, goes beyond the GDPR by requiring information on all countries to which data is exported.[23]

Unlike the GDPR, which has a more extensive list of mandatory information requirements, Art. 19 of the DSG focuses on a narrower set of criteria. These include contact details, processing objectives, types of data processed, recipient categories, international data transfers, and automated decision-making processes. Art. 19 DSG exceeds the GDPR only in specifying that not just the act of foreign data disclosure must be mentioned, but also the countries receiving the data, although a general designation of country groups or regions is acceptable.[24]

B. More Flexibility

The flexible nature of Art 19 DSG leaves room for proportionate information and avoids undue informa-

17 See Chapters IV and V below for more details; David Rosenthal (fn. 2), p. 38; Kurt Paerli/Nathalie Flueck (fn. 1), p. 237 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 42.

18 According to Art. 5(e) DSG, "disclosure" means not only the transfer but also any access to personal data from abroad, which includes the use of cloud-based services.

19 David Rosenthal (fn. 2), p. 38; Kurt Paerli/Nathalie Flueck (fn. 1), p. 239 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 32 et seq.

20 For example, it is sufficient to refer to a standard contractual clause recognised by the European Commission and the FDPIC, which is by far the most common instrument for safeguarding cross-border data transfers; David Rosenthal (fn. 2), p. 38; Kurt Paerli/Nathalie Flueck (fn. 1), p. 239 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 32 et seq.

21 See Chapters IV and V below for more details.

22 Art. 13(1)(c), (2)(a-d) GDPR.

23 Art. 19(4) DSG; Kurt Paerli/Nathalie Flueck (fn. 1), p. 237.

24 Matthias Glatthaar/Annika Schröder (fn. 3), n. 33.

tion overload, so that information can be tailored to the relevant data on risk, thereby omitting extraneous details.[25] Information exceeding the minimum requirements of the DSG must only be provided if necessary to ensure appropriate and transparent data processing (Art. 19(2) DSG). This is likely to be the case when the data are sensitive, the processing extensive and the more unusual the technologies used for the processing. In each case, the guiding principle is what data subjects need to know in order to be able to exercise their rights. The requirements of the GDPR should provide an upper limit in this respect.[26]

The importance that the duty to inform does not become an excessive burden for data controllers and remains limited to cases where it is necessary for the protection of the data subject's interests is also reflected in the newly defined catalogue of exceptions under Art. 20 DSG. According to Art. 20(1)(a), a data subject does not have to be informed about something he or she already knows. Therefore, if there is relation in time and content between the previous and current data collection, the data controller is not required to provide the data subject with new information. Where individuals provide their personal data to a company without any involvement (e.g. by sending an unsolicited email request) they are deemed to have been informed in advance. Therefore, if the circumstances indicate that the data subject has waived the right to information pursuant Art. 19 DSG, or if they are not interested in the information, they do not need to be informed. This also applies in part under the GDPR. Furthermore, there is no obligation to provide information in the case of data processing required by law (Art. 20(1)(b)). Data controllers benefit from this exception if a provision of Swiss law requires data processing.[27] Other exceptions may be justified by professional secrecy and the protection of sources in media work (Art. 20(1)(c) and (d) DSG). In the case of indirect data collection, the duty of information may be waived if the data controller cannot inform the data subject because the effort to identify and locate the individual or to provide the information itself would be disproportionate (Art. 20(2) DSG). The determination of proportionality requires an assessment of the relationship between the burden on the data controller and the interest and need of the data subject to obtain the information. In cases involving many data subjects, an individual assessment is not necessary and generalisations can be used instead.

Finally, Art. 20(3)(a) DSG provides that the duty of information may be waived or delayed in part or completely, depending on a balance of interests. Such an exception applies when the interests of third parties would be impaired by the information, for example, when the information contains personal data of third parties or when the disclosure of the information would jeopardise the primary purpose of data processing and this purpose outweighs the immediate need for information. An example would be in pharmacovigilance, where the greater public interest may necessitate sharing data with authorities to address safety concerns about medicinal products. However, according to literature, this provision should be interpreted restrictively and information should be limited only if strictly necessary. In principle, the solution that is more favourable to the data subject should be chosen, ensuring the most transparent data processing possible in the circumstance.[28] Therefore, pharmaceutical companies should invoke Art. 20(3)(a) DSG sparingly and only with explicit regulatory guidance.

C. Conclusion

In practice, it is advisable for larger and internationally oriented companies to go beyond the mandatory information requirements and comply with the generally more comprehensive GDPR. This is also because their data processing could fall within the scope of the GDPR. In particular, the GDPR catalogue also requires information to be provided on the storage period, the applicable legal basis, the legitimacy of the interests pursued, the rights of the data subjects and the right of appeal.[29] Nevertheless, especially pharmaceutical companies should be aware of the flexible regulation of Art. 19 DSG and its exceptions according to Art. 20 DSG.

IV. Data Privacy in Application of Reimbursements in Individual Cases: Navigating the Complexities of the Revised DSG

The reimbursements for the cost of medicinal products in individual cases according to Art. 71a-d of the Ordinance on Health Insurance (hereinafter "KVV") serve as essential avenues for patients to access treatments that are not yet commercially available or are unlicensed in a particular jurisdiction. However, the data privacy dimensions of such cases, especially in the context of the revised DSG, warrant careful attention.

A. Obligations Under Article 19 DSG

Art. 19 DSG constitutes a crucial provision of the DSG in the context of individual reimbursements,

25 Matthias Glatthaar/Annika Schröder (fn. 3), n. 19.
26 Matthias Glatthaar/Annika Schröder (fn. 3), n. 37 et seq.
27 This will be further discussed in Chapter V(B) below.
28 BBl 2017 7053 et seq.; David Rosenthal (fn. 2), p. 40 et seq.
29 It is also important to note the difference in penalties. Unlike the DSG, the GDPR fines of up to EUR 20 million or 4% of the global annual turnover (Art. 83(5) GDPR) are primarily directed against the company, rather than the natural persons acting on behalf of the company; Matthias Glatthaar/Annika Schröder (fn. 3), n. 36, n. 74.

which mandates entities to apprise individuals at the point of collecting their personal data. Pharmaceutical companies, in their interactions with health insurance entities, often receive personal data – sometimes even clear-text full names of patients – although they never requested such level of details.
In such cases, the requirements under Art. 19(2) and (3) DSG must be complied with by informing the data subjects about the indirectly obtained data and the subsequent data processing activities.[30] With regard to internal processing and disclosure at pharmaceutical companies, it should be noted that health data is considered particularly sensitive personal data pursuant to Art. 5(c)(2) DSG. Accordingly, pharmaceutical companies should ensure that the processing principles pursuant to Art. 6 DSG are observed. In particular, personal data may only be processed in such a way that the processing is compatible with the identifiable purpose of the collection (purpose limitation). In addition, the processing must always be proportionate. Accordingly, the data may only be viewed and processed by persons who are responsible for fulfilling the procurement purpose.[31]

B. The Challenge of Inconsistent Consent Practices

The DSG envisions a framework where treating physicians and health insurance companies secure prior patient consent before transmitting personal data. The attending physician is obliged to obtain the patient's consent before forwarding sensitive data to health insurance companies or pharmaceutical companies. Similarly, health insurance companies must secure patient consent before sharing any patient data. In cases, where patients have already been informed about the data processing for the reimbursement demand and have given their consent to the health insurance company or the physician, the data processing by the pharmaceutical company would be covered by the consent and exempted from the duty to inform in accordance to Art. 20(a) DSG.
Yet, realities on the ground indicate lapses in this practice. The repercussions are twofold: patients' rights might be compromised, and pharmaceutical companies might inadvertently breach data protection norms.

C. Proactive Engagement and Collaboration

To avoid potential legal and ethical pitfalls, a proactive approach is crucial. Pharmaceutical companies should ensure that their data privacy policies contain the appropriate information as required by the DSG standard. As formal data protection agreements with health insurers and physicians are not mandatory, it is highly advisable to request their confirmation that they have obtained the data subject's consent for the relevant data processing involving the pharmaceutical company. If it is uncertain whether requisite consents have been obtained, data should be transmitted in an anonymized or pseudonymized format. Additionally, communication protocols should be established with physicians to ensure data is shared responsibly.[32]

D. Incorporating Specific Notices in Online Privacy Policies

An additional layer of protection can be introduced by pharmaceutical companies in their online privacy policies. Due to the obligation to provide information under Art. 19 DSG, it is advisable for pharmaceutical companies to adapt the data privacy policy on the website by including a specific notice stating that patient data will be processed in the context of individual compensation pursuant to Art. 71a-d KVV. Specifically, the policy should contain all the information required by Art. 19 DSG.[33] This allows both physicians and patients to easily access relevant information on the company's website. In this way, pharmaceutical companies can provide clarity to patients and strengthen their own data protection measures to mitigate risks.

E. Conclusion

Reimbursements in individual cases are invaluable for patient care but come with intricate data protection complexities. With the revised DSG now in play, pharmaceutical companies must be vigilant in adapting their practices. By doing so, they can continue to serve the best interests of patients while ensuring rigorous compliance with data protection standards.

V. Necessary Content of Data Privacy Notices: A Focus on Pharmacovigilance

In the evolving landscape of data protection, the pharmaceutical sector, with its emphasis on pharmacovigilance, stands at a critical juncture. The intricate balance between safeguarding individual rights and ensuring public health necessitates robust data privacy mechanisms. Here, we delve deeper into how to navigate new challenges, particularly in the realm of pharmacovigilance.

A. Challenges and the Need for Data Privacy Notices

In the context of pharmacovigilance, companies may obtain personal data directly from data subjects (e. g.

30 See Chapters II(B) and (C) for more details.
31 David Rosenthal (fn. 2), p. 14 et seq., p. 38; Kurt Paerli/Nathalie Flueck (fn. 1), p. 240; Matthias Glatthaar/Annika Schröder (fn. 3), n. 19.
32 David Rosenthal (fn. 2), p. 39; Kurt Paerli/Nathalie Flueck (fn. 1), p. 237 et seq., p. 242 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 40, n. 55.
33 See Chapter II for more details; Matthias Glatthaar/Annika Schröder (fn. 3), n. 29 et seq., n. 44.

patients) or even indirectly from third parties (e.g. healthcare providers), which could be challenging if the patient's data is not first anonymised. As mentioned above, Art. 19 DSG provides for a duty to inform the data subject when obtaining personal data, especially when the data subject is unaware of the processing of the data.[34] However, complying with this obligation could require disproportionate efforts or even be impossible, as pharmaceutical companies usually do not have the contact details of patients and may not be able to locate and inform them. In such cases, the exceptions under Art. 20(2)(a) and (b) DSG may apply. In addition, the exception under Art. 20(3)(a) DSG could be relevant, as third parties may have an overriding interest in pharmacovigilance information being processed and made available to the authorities and the broader public. The duty to provide information could also be unnecessary and disproportionate if the data transfer is obvious, or if the data subject should have been informed by the healthcare providers in the first place (Art. 20(1)(a) DSG).[35]

B. Pharmacovigilance as an Exemption

However, the exemptions mentioned above rely on a balance of interest and are therefore challenging to invoke without clear guidance by the authorities. Especially in the case of pharmacovigilance, it might therefore be more feasible for pharmaceutical companies to invoke Art. 20(1)(b) DSG: the duty to inform does not apply if the processing is provided for by law.[36] According to the literature, no specific legal basis is required for this, but it is sufficient if the data processing is part of a legal obligation.[37] Conversely, this means that this exemption from the duty to inform applies only to the extent that the processing is necessary to fulfil the underlying legal obligation. Data processing that goes beyond the legal obligations is therefore not covered by the exception and the data controller must comply with the information obligations under Art. 19 DSG when obtaining the personal data.

Pursuant to Art. 59(1) of the Therapeutic Products Act (hereinafter "HMG"), anyone who manufactures therapeutic products or distributes ready-to-use medicinal products must ensure a reporting system. The reports must be submitted in accordance with the recognised rules of good vigilance practice. According to Swissmedic's practice, the initials of the patient must be included when forwarding the reports in order to avoid duplicates. Based on Art. 59(1) HMG and Swissmedic's guidance, pharmaceutical companies are obliged to accept pharmacovigilance reports and to forward them to Swissmedic in the form provided for this purpose.[38] Consequently, Art. 59(1) HMG constitutes data processing provided for by law. Therefore, there is no obligation to inform the patient when the data is collected or obtained in accordance with Art. 59(1) HMG and Art. 20(1)(b) DSG, provided that the processing is necessary for the underlying legal obligation.[39]

The reporting system of a pharmaceutical company is usually operating internationally. For the operation of a reporting system according to Art. 59(1) HMG, it is essential that pharmacovigilance data are shared within companies of the same group. Only then can the group effectively perform the task of evaluating pharmacovigilance reports, which is necessary for a reporting system. In addition, pharmaceutical companies are each required by regulatory requirements to share these reports with foreign authorities as well. As a consequence, data from a pharmacovigilance report are regularly transferred abroad and processed there. Therefore, the transfer of data within the group within the framework of the reporting system according to Art. 59(1) HMG must also constitute data processing provided for by law, which is why the exception under Art. 20(1)(b) DSG applies in such cases.

C. Limits of the Exemption and Risk Reduction

It should be noted that any data processing that goes beyond the obligation under Art. 59 HMG is in principle subject to the information obligation under Art. 19 DSG. In order to determine whether the data processing takes place within or outside the provision of Art. 59 HMG, the general processing principles pursuant to Art. 6 DSG must be observed.

For the processing of personal data in the context of pharmacovigilance, the principles of proportionality (Art. 6(2) and (4) DSG) and purpose limitation (Art. 6(3) DSG) are particularly relevant. The principles of proportionality and purpose limitation require that the data may only be viewed by competent persons and may only be processed to the extent necessary to fulfil the pharmacovigilance obligations. Accordingly, it is recommending to restrict access to those employees who are responsible for processing the pharmacovigilance reports. In addition, care should be taken to ensure that personal data is only processed for the purpose of the reporting system and not used for other purposes.[40]

34 See Chapter II(C) for more details.

35 See Chapter III(B) for more details on the exceptions under Art. 20 DSG; David Rosenthal (fn. 2), p. 40 et seq.

36 Art. 20(1)(b) DSG; David Rosenthal (fn. 2), p. 38; Kurt Paerli/Nathalie Flueck (fn. 1), p. 237 et seq.; Matthias Glatthaar/Annika Schröder (fn. 3), n. 42.

37 Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 20 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version 20.8.2023, n. 13, available at: https://onlinekommentar.ch/de/kommentare/dsg20.

38 See https://www.swissmedic.ch/swissmedic/en/home/humanarzneimittel/market-surveillance/pharmacovigilance.html.

39 David Rosenthal (fn. 2), p. 40 et seq.

40 David Rosenthal (fn. 2), p. 14 et seq.

However, it should be added that the assessment of whether data processing or data transfer takes place within or outside of the scope of Art. 59(1) HMG can be difficult and must be assessed on a case-by-case basis.[41] Therefore, in order to mitigate the risk in relation to data protection, it may be advisable to provide additional data privacy notices to patients for pharmacovigilance reports.

D. Conclusion

Navigating the intricacies of data privacy in pharmacovigilance is a vital aspect of pharmaceutical operations. Regulatory compliance is not merely a legal formality but a key factor that safeguards both the company and the data subjects involved. Our discussion has highlighted that some data processing activities may be exempt under Art. 59(1) HMG; however, it's critical to recognize the limitations of these exemptions. Adherence to Art. 19 DSG and Art. 6 DSG serves as a cornerstone for maintaining robust data protection protocols. By crafting transparent and comprehensive data privacy notices, pharmaceutical companies can mitigate risks, ensure regulatory compliance, and maintain a reliable reputation in this highly sensitive domain.

VI. Final Thoughts

The interplay between data privacy and the pharmaceutical sector is nothing short of a constantly evolving landscape. As we have journeyed through the specificities of Art. 19 DSG in the context of pharma websites, scrutinized the detailed prerequisites for data privacy notices, and navigated the unique challenges posed by individual reimbursements and pharmacovigilance, several salient points crystallize.

First and foremost, the revised DSG, aimed at aligning Switzerland's data privacy norms with international standards, has ushered in an array of unique challenges for the pharmaceutical sector. This goes beyond mere compliance checkboxes; it's about sustaining and fortifying the trust vested by patients, healthcare professionals, and the general public.

Second, the convoluted processes involved in data collection and dissemination, especially in specialized programs, accentuate the critical need for robust, transparent, and comprehensive data protection strategies. These are not merely legal requirements; they are essential elements of ethical business conduct in the pharmaceutical industry.

Lastly, the role of collaborative efforts and proactive engagement can't be overstated. Pharmaceutical companies must ensure that they comply with new requirements and, where their duty to inform may not be fully met, obtain confirmation of the necessary consent from healthcare providers or insurance companies. Therefore, as the norms around data protection continue to evolve, a cohesive approach will be vital for ensuring not only regulatory compliance but also the centrality of patient welfare and innovative therapeutics.

In essence, the revised DSG, while introducing a new set of challenges, also provides an opportunity for pharmaceutical companies. It serves as a catalyst for these entities to reaffirm their commitment to data protection, increase operational transparency, and strengthen stakeholder trust.

41 Kurt Paerli/Nathalie Flueck (fn. 1), p. 241.