Monthly
Newsletter
November 2022

Data

Implementation of the New Data Protection Act: Step 2 - External Measures

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

1.
Existing privacy notices are to be reviewed, and additional privacy notices have to be implemented for target groups not previously covered.

2.
The access right (right to information) is specified and will be subject to a stricter sanctions regime. Accordingly, the relevant processes and templates should be reviewed and updated.

3.
In case of cross-border transfers, the EU standard contractual clauses will be applied in most cases, supplemented by a Swiss Rider with the necessary adaptations to Swiss law.

1 Overview

The new Data Protection Act (nDPA) and the new Data Protection Ordinance (nDPO) will come into force on 1 September 2023. In our October 2022 newsletter, we outlined a **three-step roadmap** and set out the first step in more detail. In this newsletter, we focus in step 2 on the measures with external effects. We will deal with the internal measures (step 3) in the next newsletter.

The suggested roadmap may serve as a guide, but must be adapted to the specific situation and individual starting point and, to the extent necessary, must be supplemented with industry- and sector-specific characteristics. Particularly in the implementation of externally effective measures the focus will depend heavily on the respective **business area** and on **internal requirements** of the company or group.

With a focus of step 2 on the **measures with external impact** and possible sanction consequences, we address the following topics:

— Duty to inform and privacy notice
— Access right
— Cross-border transfers

Information on the roadmap and timetable can be found in our October 2022 newsletter. Regarding existing cross-border transfers, the deadline for replacing the standard contractual clauses (**SCC**) based on the "old" templates **by the end of 2022** must be observed (see section 4.2).

2 Duty to Inform and Privacy Notice

Under current law, it is sufficient if the data collection is recognizable from the circumstances; active information is only necessary in exceptional cases. Under the nDPA, a **duty to inform applies in principle to all data subjects**, unless an exception applies: accordingly, the duty to inform does not apply, inter alia, if the data subjects **already have the relevant information** or if the processing is **provided for by law**. For example, it is not necessary to provide the information each time in case of repeated data collections. The exception of processing provided for by law includes, for example, the collection of employee data insofar as this is only carried out to fulfill legal obligations (such as the preparation of salary statements (*Lohnabrechnung*)). If additional data is collected or existing data is processed for additional purposes, this would then again be subject to the duty to inform.

The type and manner of information can in principle be chosen freely. Usually, the information is provided in the form of a **privacy notice**.

2.1 Who Must be Informed?

If a collection takes place in an intentional and planned manner, **all persons affected by the data collection** must be informed: If one is given a business card spontaneously or receives an unsolicited e-mail, this will not suffice to trigger the duty to inform - the targeted collection of contact data at a trade fair stand or a contact form on a website, on the other hand, will trigger it.

After identifying the **various target groups** (such as customers, service users, employees, supplier contacts, etc.), it must be determined **which data** regarding these target groups is processed and **for what purposes**. Then it must be decided whether **several individual privacy notices** should be set up for each different target group (leading to shorter and more precise privacy notices) or whether **one privacy notice** should cover all target groups and all data processing (which can simplify certain processes).

All persons affected by the data collection must be informed.

2.2 How Does the Information Have to be Provided?

The information must be provided **at the time of collection**. If the data is not obtained from the data subject (but e.g. from third parties or from generally available sources), the information must be provided **within one month** at the latest or, in the case of prior disclosure to a recipient, at the latest **at the time of such disclosure**. With regard to the type and manner of information, the nDPO only stipulates that this must be provided "**in a precise, transparent, comprehensible and easily accessible form**".

It is thus not necessary to hand over a privacy notice or display it in full for every data collection. It is sufficient if the data subject's attention is drawn to the privacy notice and it is made easily accessible. For example, a **comprehensive privacy notice may be available on a website**, with the data subjects **receiving a reference** to it in a transparent manner (e.g. by a link, QR code, an announcement preceding a telephone call etc.).

2.3 What Does the Information Have to Contain?

In contrast to the fixed catalog according to the EU General Data Protection Regulation (**GDPR**), the nDPA contains a **general clause** according to which the data subject must be provided with the information "that is necessary to enable him/her to assert his/her rights under this Act" and to "ensure transparent data processing". Depending on the situation, the necessary scope of information may thus be narrower or broader. In any case, however, the following **minimum information** must be communicated:

— Identity and contact details of the data controller;
— Purpose of processing;
— Categories of recipients to whom personal data is disclosed;
— Categories of personal data processed (if the data is not obtained from the data subject); and
— in the case of cross-border transfers, the target countries and, if applicable, the relevant safeguards implemented (most likely SCC, cf. Section 4.1).

Depending on the type of data and the nature and scope of the data processing (e.g. in the case of several data controllers or complex data combinations), **additional information** may be required on the basis of the general clause (e.g. on the

data source or regarding specific recipients). Explicit information must also be provided in the case of automated individual decisions (**AID**), and in such case additional processes must be implemented as well.

2.4 Implementation Remarks

Existing privacy notices should be reviewed to determine whether they contain the required **minimum information** or whether **additional information** may be necessary. For target groups not yet covered by an existing privacy notice, **new privacy notices** must be implemented (or existing privacy notices amended). It must be ensured that data subjects are **made aware of the privacy notice** in an appropriate manner and can access it easily. If **GDPR compliant privacy notices** are already in use, they can serve as a basis, but must be amended in particular in case of cross-border transfers with the information on the target countries (and, if applicable, the safeguards implemented).

The privacy notices should be addressed with priority, as they represent the **direct point of contact with data subjects** and failure to comply with the information obligation may be sanctioned with a **fine**.

The assertion of the access right does not require justification.

3 Access Right / Right to Information

3.1 Assertion and Content

Compared to the current law, the nDPA specifies the **access right**, with which data subjects can request information regarding the data processed about them (*Data Subject Access Request*, **DSAR**). **No justification** is required for the assertion of this right.

In terms of content, a response to an access request comprises the information that must already be contained in the privacy notice (cf. Section 2.3), supplemented by the data processed in the specific case as such and information on the retention period (or the criteria for its determination) as well as on the data source, insofar as such data was not obtained from the data subject itself.

3.2 Restrictions

The information may be **limited**, in particular if provided for by law (e.g. to protect professional secrecy), in the case of prevailing interests of third parties (e.g. if it would be possible to draw conclusions about other data subjects), if the request is of a contentious nature or serves a purpose inconsistent with data protection (e.g. mere evidence discovery).

In addition, the controller may also limit the information if its **own overriding interests** so require, provided it does not disclose the data to third parties.

3.3 Form, Timeline and Costs

In principle, the **information** must be provided in **text form** and may also **be transmitted electronically**. The data controller is **obliged to identify** the person requesting the information and such person is obliged to cooperate in this regard.

As under current law, the information must be provided **within 30 days** and **free of charge**; only in case of a disproportionate effort, the controller may levy a fee (up to a maximum of CHF 300).

SCC based on the "old" templates have to be replaced before the end of 2022.

3.4 Implementation Remarks

Even though little changes compared to the current law, the **processes and templates for responding to access requests** should be reviewed in light of the more specific requirements in the nDPA, especially since a breach of the duty to provide information may now be sanctioned to a much greater extent and with significantly higher fines (up to CHF 250,000). GDPR-based templates may be used, but must be amended in particular with information on target countries and safeguards implemented (cf. sections 2.3/2.4 above).

4 Cross-Border Transfers

4.1 Few Changes to the Current Law

If data is disclosed abroad, it needs to be verified according to **Annex 1 to the nDPO** whether the target country has an adequate level of data protection. If this is not the case, a risk assessment (so-called ***Transfer Impact Assessment*** **(TIA)**) must be carried out, similar to a data protection impact assessment, and appropriate safeguards must be implemented, usually by use of **SCC, adapted to Swiss law with a "Swiss Rider" (CH-SCC)**. In principle, there are no changes compared to current law, except that under the nDPA the conclusion of the CH-SCC no longer needs to be notified to the Federal Data Protection and Information Commissioner (**FDPIC**), provided that the EU-SCC recognized by the FDPIC are used with the necessary amendments for Swiss law.

However, the **due diligence obligations in connection with cross-border transfers are now subject to the stricter sanctions regime of the nDPA**. For example, anyone who intentionally transfers data to a country without adequate data protection without having implemented the necessary safeguards (e.g. CH-SCC) may be fined.

4.2 Replacement of existing SCC

Regardless of the implementation of the requirements of the nDPA, existing SCC concluded on the basis of the "old" standard contractual clauses must be replaced **by the end of 2022**

according to the instructions of the FDPIC. Further details on this can be found in our newsletter of May 2022.

4.3 How to Proceed Regarding New SCC

The obligation to implement appropriate safeguards in case of cross-border transfers to countries without adequate data protection has been made subject to sanctions under the nDPA. Thus, in a first step, the **cross-border transfers (and target countries) should be identified** and, in a second step, addressed where necessary by means of suitable instruments (such as e.g. **intra-group data transfer agreements (IGDTA)** in group-internal situations or **CH-SCC** regarding data recipients outside the group).

Even though there is currently a development to set up a new data protection framework regarding data transfers between the EU and the USA, it would hardly be advisable to rely solely on this in the short and medium term: Until it can be assessed whether and to what extent the newly proposed "**EU-U.S. Data Privacy Framework**" will endure and also be applicable for Switzerland, it is advisable to continue to rely on safeguarding cross-border data transfers to the USA by means of CH-SCC and TIA.

5 Outlook and Conclusion

Shortcomings in the implementation of the measures with external effects, as outlined above, can have consequences not only in the form of reputational damage but can also, under certain circumstances, lead to sanctions in the form of fines.

The implementation of the measures regarding the **duty to inform**, the **access right / right to information** and regarding **cross-border data transfers** should therefore be addressed without delay. The further need for action regarding the implementation of internal measures will be addressed in the next newsletter.

Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch

Dr. Samuel Klaus
Partner Zurich
samuel.klaus@swlegal.ch

Vincent Carron
Partner Geneva
vincent.carron@swlegal.ch

Dr. Catherine Weniger
Counsel Geneva
catherine.weniger@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P. O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.ch

Geneva
15bis, rue des Alpes
P. O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.ch

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg