Privacy in M&A transactions

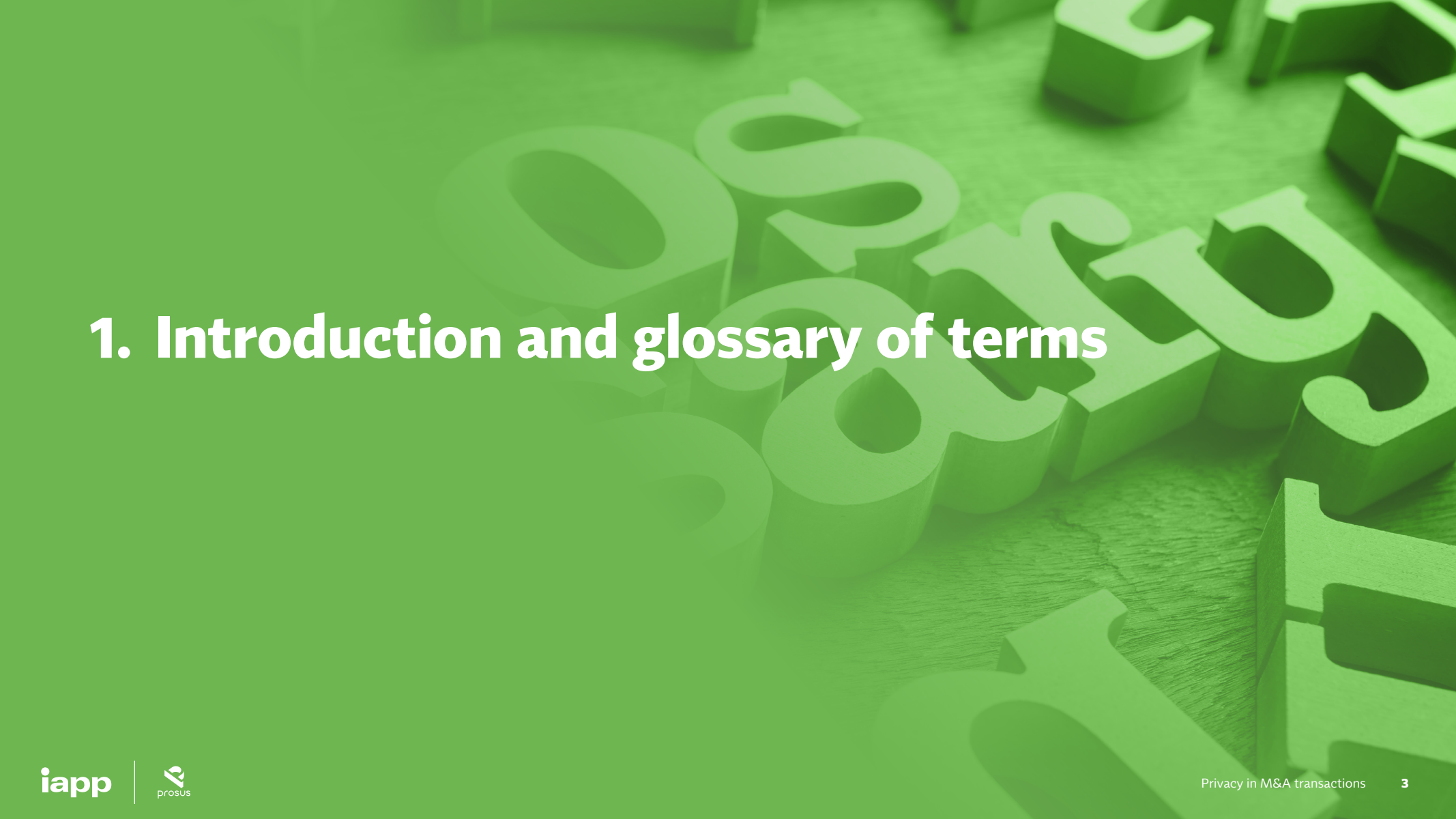
The playbook

Table of contents

Author

Marcin Czarnecki, CIPP/E, senior privacy counsel, Prosus, marcin.czarnecki@prosus.com
Co-author, Justin B. Weiss, CIPP/A, CIPP/E, CIPP/US, CIPM, FIP, global head of data privacy, Naspers & Prosus, justin.weiss@prosus.com

1. Introduction and glossary of terms



Why an M&A playbook for 'privacy'?

Mergers and acquisitions has been central to us for a long time. Given our group emphasis on the importance of privacy in data-centric transactions, consideration of data protection and other associated issues in an M&A context is essential. However, unlike employment or IP matters, teams across the group may lack well-established precedents for how to approach privacy risks that arise in M&A. This playbook aims to address this need by consolidating our group's experiences and learnings to date in this domain.

Who is this playbook for?

The playbook is directed to **M&A teams** and **privacy teams** alike. For M&A team members, it is a chance to broaden their knowledge to help identify potential privacy-related issues themselves (especially if a privacy specialist is not brought over the wall). Privacy team members will learn how to navigate the M&A process and add value as an essential stakeholder.

How to use this playbook?

The playbook is not intended to be a legal document that sets mandatory policy. It contains some suggestions and examples based on past experiences; therefore, it is designed as an **information and training tool**.

Glossary of M&A terms

APA means an asset purchase agreement, which is a legal document on the basis of which assets are sold in an asset transfer transaction.

Seller or **vendor** means the entity that intends to sell the target business to the purchaser.

M&A means mergers and acquisitions.

Purchaser or **buyer** means the entity that intends to acquire the target business from the seller.

Red-flag due diligence (report) means a review and report that focuses on matters crucial for the transaction, in particular, main risks (unlike a full report that contains a description of all aspects of the target's operations).

Data room or **virtual data room (VDR)** means an online space where due diligence documents are made available for review. Historically, data rooms were physical rooms containing hard copies of documents.

Glossary of M&A terms

SHA means a shareholders' agreement, which is a legal document setting out shareholders' contractual arrangements, including the terms on which they can sell their shares.

VDD means a vendor due diligence review.

SPA means a share purchase agreement, which is a legal document on the basis of which shares in a target are sold in a share transfer transaction.

Target/target business means a company or companies whose shares (in a share transfer transaction) or assets (in an asset transfer transaction) are to be transferred as a result of the transaction.

TSA means a transitional services agreement, which is a legal document based on which certain services provided to the target by the seller or its group will continue to be provided for a specified time following completion.

Transaction team means the M&A counsel and the business persons leading the transaction process.

Glossary of privacy terms

C

Consent or choice means the idea that consent must be freely given, specific and informed and that data subjects must have a genuine choice as to whether to provide personal data.

Controller means a natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data.

D

Data subject means an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly — in particular, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

DPA means a data processing agreement, which is an agreement setting out the terms on which a processor processes personal data on behalf of a controller.

DSRs mean data subject rights, that is rights of individuals in relation to their personal data. The basic DSRs include right of access to personal data, right to correct data and right to have the data deleted. Depending on the jurisdiction, the catalogue of DSRs may be much wider.

Data mapping means keeping records of personal data processing operations describing such aspects as data controllers, purposes, categories of personal data, processors and recipients of data, etc.

Glossary of privacy terms

I

International data transfer restrictions mean restrictions set out by data protection laws of various countries setting out specific requirements for transfers of personal data outside the territory of such countries or requirements relating to the localization of certain categories of data. Countries having such restrictions include, for example, the European Union member states, India, Brazil and Russia.

P

Processor means a natural or legal person other than an employee of the data controller or other body that processes personal data on behalf of the data controller.

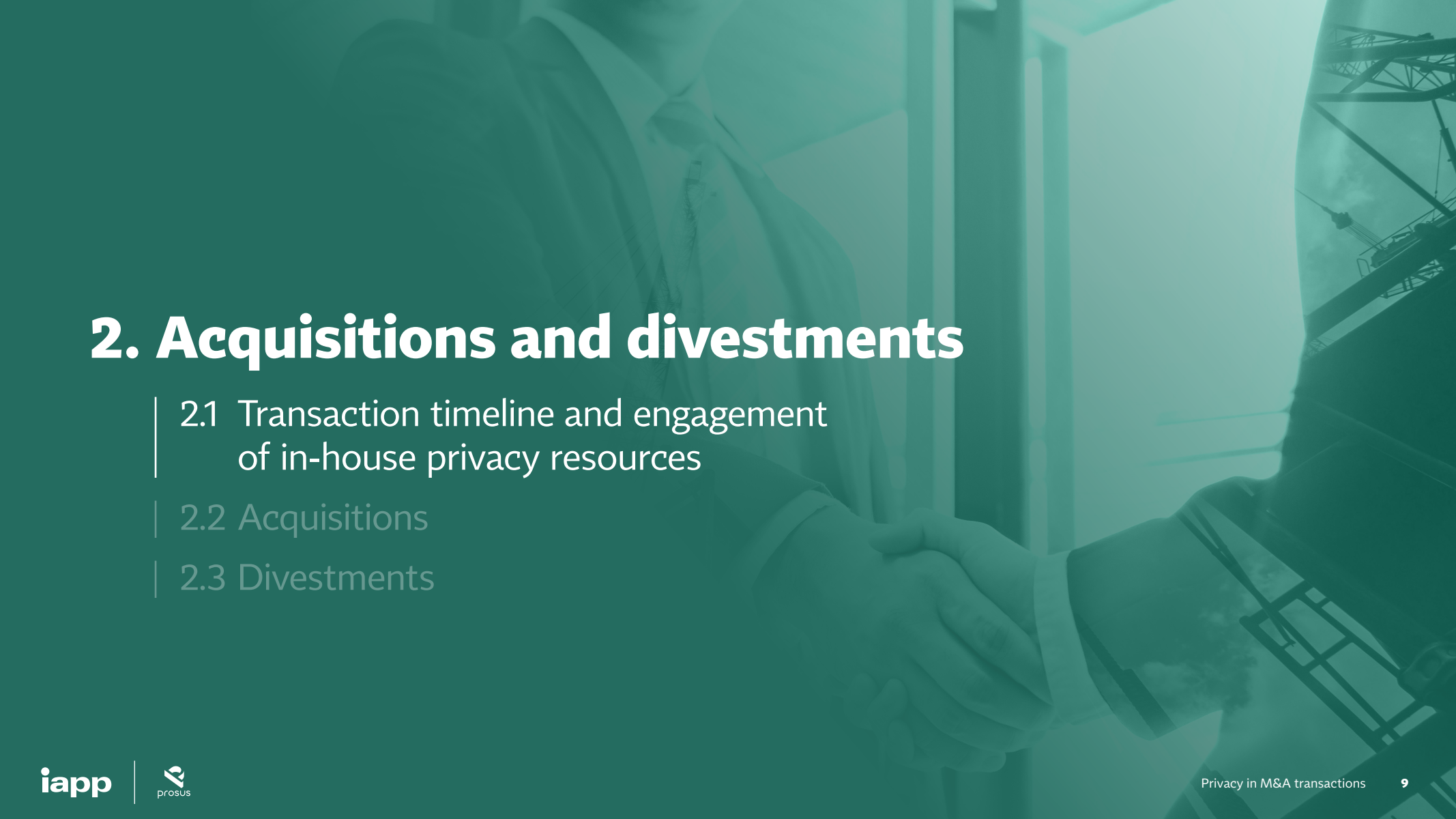
Privacy notice or **privacy statement** means a statement made to a data subject that describes how an organization collects, uses, retains and discloses personal data.

Personal data means any information relating to an identified or identifiable natural person.

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately.

S

SCCs mean standard contractual clauses, a set of contractual clauses adopted by the European Commission by which organizations can commit to protect personal data to facilitate cross-border personal data transfers and address the international data transfer restrictions.



2. Acquisitions and divestments

Transactions timeline

M&A transactions usually have a structured timeline. Specific phases of a typical transaction are outlined in the graph below together with information about main actors and deliverables. Note that frequently business and M&A teams may refer to transaction as all the steps up until completion. However, in this playbook, we outline post-completion as part of the entire M&A process due to its correlation with actions taken pre-completion and significance of the post-completion phase for privacy compliance.

Preparations	Pre-transaction discussions	Due diligence	Negotiations	Signing	Fulfilment of completion conditions	Completion	Integration separation transitional services
Phase during which the **seller** prepares the target for sale, prepares data room and prepares VDD.	**Seller** performs marketing of the target. **Both** the seller and potential purchaser(s) discuss the details of the process.	**Purchaser** performs the due diligence and prepares a due diligence report.	**Both** parties negotiate transactional documents, such as the SPA, SHA and TSA.	**Both** parties sign the sale agreement. Note: If there are no pre-completion conditions, signing has the effect of completion and the transaction ends.	The responsible party depends on the type of condition. Most frequently, it is the anti-trust clearance that needs to be obtained by the purchaser.	On completion, the target transfers to the **purchaser**. Frequently, **both** parties need to sign additional documents.	**Purchaser** integrates the targets with its business. If target needs separation, **seller** separates the business and provides transitional services.

Transaction structures

Not all M&A transactions are created equal. It is important to recognize there are different structures for transactions, which may have an implication for the nature of work that must be done pre- and post-closing, as well as the type of contribution expected of the in-house privacy resource.

Share transfer

Share transfer takes place if shares in the target company or companies are transferred to the purchaser. Depending on number of shares held, the purchaser may become a minority shareholder or take over the control of the company (which, on a sidenote, does not necessarily mean the purchaser needs to have majority of shares). Target company carries legacy liabilities for all its data protection practices; this may include liability for data breaches. In principle, there is no need to notify or require consent from from data subjects to the transfer. However, notification or consent might be necessary for sharing target customers' and employees' data with the purchaser's group.

Asset transfer

An asset transfer transaction may include a transfer of specific assets or even an entire enterprise (e.g., business unit) from one entity to another. As a rule, the purchaser does not inherit legacy liabilities and those remain with the seller. However, if transfer of an enterprise is involved, in certain jurisdictions, the purchaser may be held jointly and severally liable for legacy liabilities of the enterprise. Take this into the account when setting the scope of the due diligence. Transfer of personal data usually requires additional conditions to be met – from notification to data subjects' consent. In some jurisdictions, additional registrations or regulatory consents may be necessary.

Merger

A merger results in two companies becoming one – either by one company absorbing another or by creating a new entity that absorbs both merging companies. Similar to share transfer, the merged company inherits all legacy liabilities for data protection practices. Although the merged companies become one, there might be some additional notifications or consents needed to use customer personal data of one merging company's business unit for the purposes of the other merging company's business unit.

Basic approaches to privacy resource engagement

In M&A transactions, the transaction team coordinates the process and decides if and when to engage stakeholders. This is due, in part, to the confidential nature of such transactions. The descriptions below present an "ideal world" framework for in-house privacy resource engagement by a transaction team. As these are guidelines, different arrangements can be applied by the transaction team; in such case, it is up to the transaction team to communicate its expectations to the internal privacy resource.

Involvement of an in-house privacy resource

The transaction team may bring an internal privacy resource over the wall to perform or review reports of the due diligence, suggest questions, indicate compliance gaps and recommend risk mitigations. If the transaction team has not brought an internal privacy lawyer over the wall in the early stage, they may do so at any of later stages.

Internal or external due diligence

The transaction team should choose whether the privacy part of the due diligence is performed by an external law firm or the in-house privacy resource. If due diligence is performed by an external law firm, the in-house privacy resource could be engaged to review the DD questionnaire, suggest supplemental questions and review responses.

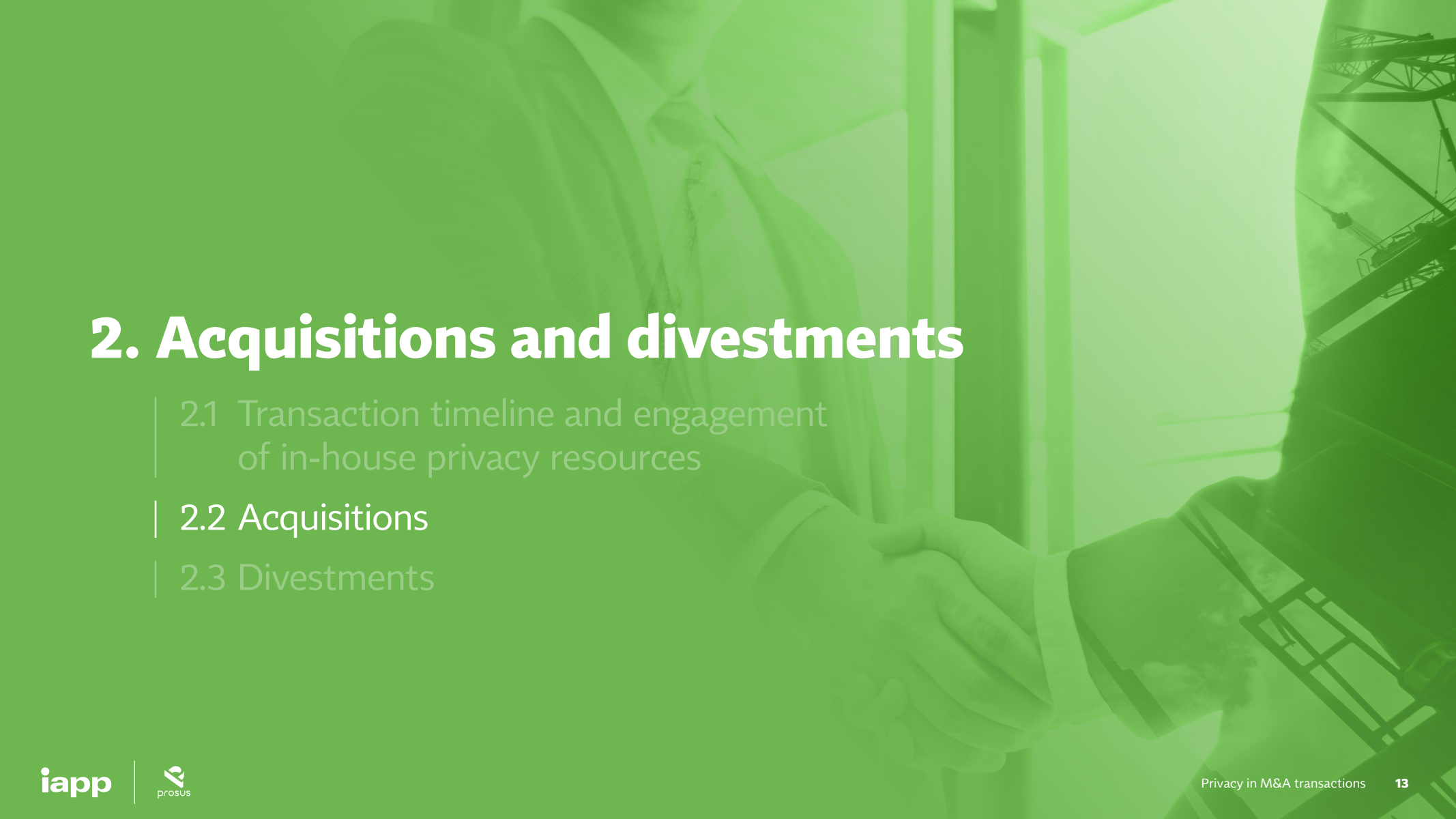
Risks and mitigation measures

Based on the due diligence, a privacy resource involved in the transaction:

- Indicates compliance gaps that appear to create material risks.
- Recommends a set of mitigation measures.
- In the case of divestments, responds to the purchaser's requests related to privacy.

In-house privacy resource support during post-completion

In most cases, in-house privacy resource support will be required to assist the target business following completion with delivering post-completion conditions, onboarding and integration with the privacy program of the relevant business and, in the case of divestments, separation of the divested business.



2. Acquisitions and divestments

Due diligence — How to prepare

Due diligence is most commonly the first stage when privacy function gets engaged in an acquisition transaction. The objective of due diligence is to identify risks related to the acquired business or obstacles in operating the business after completion. During due diligence, make sure to take into the account the broader transaction context and the specifics of the business, including:

Business model of the target

Think what kind of personal data processing is key for the target business and whether the business model creates any new privacy risks compared to the existing business model of the purchaser's business.

Applicable privacy laws

Check what privacy laws may be applicable to the target business's operations and whether the target complies with them. Consider if any new laws would apply to the target after the transaction, e.g., as a result of integration. The EU General Data Protection Regulation is a typical example of a regulation that may be applicable to businesses that do not have any corporate presence in the EU but target users in the EU.

Use of data after transaction

Discuss with the business team whether any changes to the business model of the target are contemplated and how will this affect personal data processing. Think how the target's data will be used. For example, it might be contemplated to use the target's data to promote services of the acquiring company — this could require obtaining consents from individuals.

Transaction structure

Consider the impact of the proposed transaction structure on personal data processing operations. It is not uncommon to change the transaction structure to keep users' authorization to perform certain processing activities, in particular, in the area of marketing. See page 11 for an overview of transaction structures.

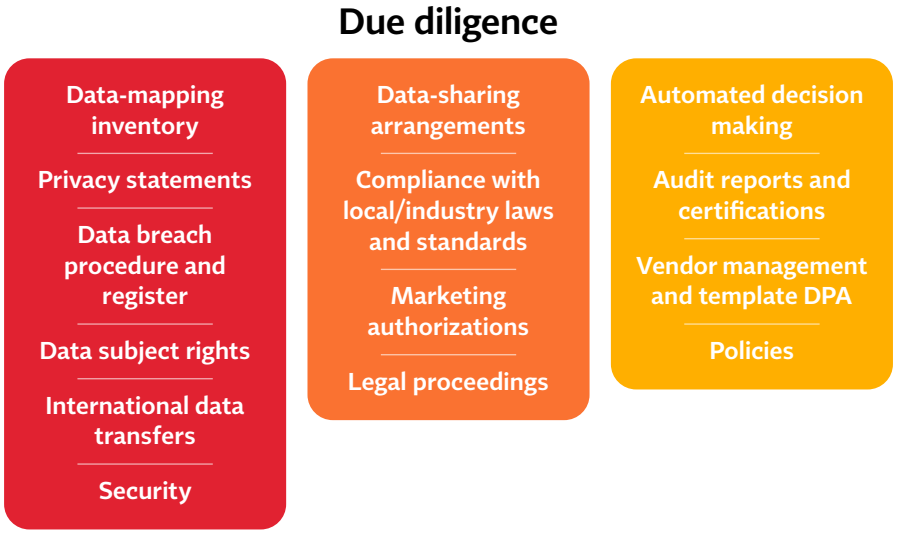
Purchaser's standards

Check how the target's privacy program benchmarks against the privacy program of the acquiring business and what amount of work and capital investments would be needed to bring the target business up to its standards.

Due diligence review tips

Although there is no universal approach to due diligence, you can look at the diagram and consider reviewing the most common areas for analysis. Whether you are starting your first due diligence or are familiar with the process, consider the following tips:

- Read the information memorandum and VDD reports, if available. Not only legal and IT topics, but also other sections may be useful — e.g., the financial section can reveal data about investments made in the privacy/security area.
- Do an independent research about the target on the internet.
- Tailor the due diligence questionnaire to the specifics of the business and transaction.
- Identify areas that should be prioritized for review and risk rate them based on their potential impact on day 1 post-completion. For example, in the chart to the right, certain elements in red might correspond to the most material risks and, therefore, justify greatest focus if time is limited.
- Start the review with the data-mapping records and privacy statements if available — they should show the data-processing landscape and may immediately reveal potential gaps and issues.
- If relevant, review both the current and past versions of documents, such as privacy notices and marketing consents, as some customers may have agreed to different terms than available on a website at the time of review.



- Consider engaging a security expert to perform a security review, if not already conducted. Lack of security due diligence review is a risk itself and should be highlighted to the transaction team.
- In acquisition transactions, a majority of due diligence reports are red flag reports. Their aim is to briefly outline risks and propose solution to mitigate such risks.
- In some transactions, especially in auction sales, sellers may introduce a limit to the number of due diligence questions in which case only top priority questions may be asked.

Due diligence risks

Once privacy gaps of the target business are identified, it is critical to appropriately assess their potential impact and propose suitable actions. Below you will find a classification of risk based on the types of mitigation measures that can be applied. Certain risks may require application of mitigation measures from more than one of these categories. You are encouraged to use this classification in communication with the transaction team.

Risks that may be addressed pre-completion

Certain risks can be mitigated or even eliminated by actions taken by the seller, purchaser or by both, prior to completion of transaction. Usually, only top risks are addressed this way.

Risks that may be addressed post-completion

Certain risks cannot or do not need to be remedied prior to completion either because of the demanding transaction timeline or a lower risk priority. If mitigation measures are possible, they will be taken after completion. It is important to agree on such measures with the seller if the purchaser does not acquire 100% of the target business.

Risks that can be addressed by warranty or indemnity

SPA warranties and indemnities are aimed at allocating risks to the seller. Please see also page 17.

Risks affecting valuation

This category relates to the impact of a risk on the valuation of the target business. This means the business teams should consider the risk in their business and valuation models. Note that valuation of the target busines may be impacted even if certain mitigation measures are taken.

Risks that need to be considered by the purchaser

This is the broadest category that includes various risks that cannot be addressed but need to be taken into the account by the purchaser, e.g., proposals for new laws that may impact the target business in the future.

SPA considerations

SPA is the legal document where risks and other privacy-related requirements may be addressed in an enforceable manner. Below you can find an overview of SPA provisions that may address various privacy concerns. Note that it is not uncommon to put some of them in other documents, such as side-letters. Usually, the transaction team is responsible for drafting and negotiating all such provisions, but a privacy lawyer may be requested to verify them and/or provide input.

Representations and warranties

Representation and warranties are an assurance made by the seller that specific facts are true. They are used to fill gaps in the due diligence or give comfort with respect to facts that are not easily verifiable, such as compliance with certain regulations or lack of data breaches. Untrue representations or warranties trigger the seller's liability toward the purchaser. The minimum set of privacy representations and warranties should include confirmations related to lack of data breaches, compliance with relevant data protection laws and disclosure of practices related to sharing of personal data with third parties.

Indemnities

An indemnity is an obligation to reimburse the purchaser in respect of loss suffered as a result of specific circumstances known to the parties. In general, while warranties protect against potential (unknown) risk, indemnities allocate risk in respect of a known matter. A typical situation in which an indemnity would be applied in a privacy context is a data breach that has been discovered but with respect to which regulator proceedings have not commenced yet and the individuals did not have time to file their complaints.

Pre-completion covenants

Pre-completion covenants may cover a wide range of activities, such as performing specific actions to mitigate risks (e.g., update of privacy statement), obtaining a regulatory approval (e.g., for a transfer of a database), requiring the seller to conduct the business in a specific manner before completion (e.g., informing the purchaser about any data breaches or authority inspections) or requiring the seller to perform certain actions to facilitate migration of data after completion.

Post-completion and other covenants

Post-completion covenants represent the broadest category of covenants. On the one hand, they may relate to specific actions required from the seller to allow the purchaser to appropriately onboard the target business, including transfer of data and provision of transitional services (see page 18). On the other hand, covenants may oblige the target's executive team to implement certain privacy measures. Such an approach is recommended if the target's executive team consists of the sellers and/or if the purchaser does not acquire 100% of the target.

Transitional services

Frequently, as a result of operational dependencies between the seller and target business, the seller is required by the purchaser to provide the target with certain services, such as access to IT systems, HR services or customer service services; such services are provided for a limited time and are referred to as transitional services. Transitional services usually entail processing of personal data. The terms of processing should be set out in the TSA and/or a data processing agreement accompanying the TSA. When preparing the terms, consider addressing:

- The **roles of the parties** (controller/processor) and **categories of personal data** processed.
- The seller's obligation to **act only on instructions** of the target business.
- The seller's obligation to appropriately **separate the target's data** from the seller's other data and implement appropriate access restrictions and security measures to ensure confidentiality.
- Restrictions on **international data transfers** under applicable laws, if any.
- A process to ensure **support of the data subject requests** by the seller.
- The seller's confirmation that it can transfer personal data without any adverse impact on their structure and content.
- Seller's obligation to **erase data** belonging to the target business after the end of the transition period.
- Seller's obligation to immediately notify the purchaser and target business about any actual or alleged **data breaches** and mitigate their consequences.

Completion and actions immediately following completion

Upon completion taking place, the ownership and risks related to the target business pass to the purchaser. This means the purchaser may be required to comply with certain legal requirements immediately after completion takes place or even before completion. Below you can find an overview of the most common privacy requirements to be taken into account when preparing for completion.

Transfer of databases

Such transfers usually occur on the grounds of asset transactions. Make sure that the transfer of personal database (or access credentials to such database) is adequately secure and that any international data transfer restrictions are addressed.

Notification/registration with regulators

Some jurisdictions require that certain privacy – related registrations are made or updated within a specific time after the transaction takes place. These may relate to database registrations and DPO registrations. Make sure that you identify such requirements and that you obtain relevant documentation about past registrations from the seller.

Updates of data-mapping records

Make sure to do at least the basic updates to the data mapping records to reflect the changes resulting from the transaction, for example the change of data controller, change of the DPO, recipients of personal data (such as the purchaser's group companies).

International data transfer requirements

Depending on the jurisdiction, transfers of personal data between the target business and purchaser's group may trigger international data transfer restrictions. Make sure that if any such restrictions exist, the requirements relating to such transfers are met before the transfers occur (e.g., to address any transfers of personal data outside the European Economic Area, you may put in place an appropriate set of SCCs).

Notice to data subjects

Consider the need to provide appropriate notice or update to the current privacy notice upon completion (or even before completion) to reflect the changes occurring as a result from the transaction. This may be needed in asset transactions, share transactions (e.g., where the privacy notice refers to sharing of personal data with the seller group) and mergers.

Integration preparations timeline

Onboarding and integration projects may range from simple onboardings requiring little input from the acquiring company's privacy team to large cross-jurisdictional projects involving multiple stakeholders. In each case, it is important to remember to obtain an appropriate executive buy-in — this applies particularly to senior managers of the acquired business who may not necessarily prioritize privacy compliance and secure for an appropriate budget.

Pre-completion preparations

The privacy team and other stakeholders do not need to wait to prepare for onboarding until completion. Consider what actions will need to be taken immediately after completion, e.g., in relation to employee onboarding.

Be mindful of limitations in transfers of personal data prior to completion — consider anonymizing or pseudonymizing data and document assessments of such transfers.

Be mindful of limitations related to exchange of other business sensitive information before completion due to antitrust reasons. In case of doubt, consult the transaction team.

Integration activities require resources, specifically human resources (time, salary), IT and potential technical resources (licenses), and often project management. It is useful to anticipate these costs generally and ensure the transaction team is clear eyed about the level of investment requirement to implement the privacy requirements post-completion.

Post-completion gap assessment

Frequently, the transaction due diligence may turn out to be not specific enough to prepare a detailed privacy program integration plan. This happens usually during large, multi-jurisdictional transactions where the due diligence is limited to the most important high-level aspects of privacy compliance.

Consider conducting a detailed post-completion gap assessment of the privacy program on a country-by-country basis. The results of the assessment will help in planning remediation measures more precisely and efficiently.

Planning

Planning is the key element for integration's success. Therefore, take into the account the following:

- Defining the intended level of integration. This may range from autonomous status of the target, in which case privacy program could also be developed independently, to complete integration, which would entail full integration of privacy programs.
- Defining the priorities of integration and privacy standard that is to be achieved.
- Defining an action list on appropriate detail level, e.g., on a function-by-function and country-by-country level.
- Assessing available resources and the need for additional support.
- Setting out key performance indicators.

Integration

During integration itself, consider the following organizational arrangements:

Larger integrations will need a person to coordinate/project manage the work of various team members. Consider appointing such coordinator.

Establish appropriate communication channels — not only within the privacy stream, but also with other work-streams, such as HR, security and data. Consider setting up regular status calls.

Establish one knowledge center where all the templates and information related to integration is uploaded. This may seem obvious, but it is often overlooked.

Integration

Privacy-related integration items can cover a wide range of matters, beginning with items usually comprising parts of a privacy program and ending on support of business teams in their integration activities. Below you can find a non-exhaustive list of items that usually can be found on the integration agenda, together with some tips. Priority of these items may vary depending on the due diligence issues identified, the nature of the target business and business priorities of the seller. However, what has frequently been prioritized from the privacy perspective during our past integrations are the introduction of a data governance policy and appointment of a privacy lead (being easy wins), followed by ensuring an appropriate data security level, as well as "front-end" items, such as update of the privacy statement and ensuring a DSR process is in place.

Privacy lead designation and DPO registration

Remember that in some countries a formal DPO appointment and/or registration is mandatory.

International data transfer compliance

Although international data transfer compliance has been mentioned as one of the completion action items, note that integrations often require a fresh look at the specifics of transfer arrangements.

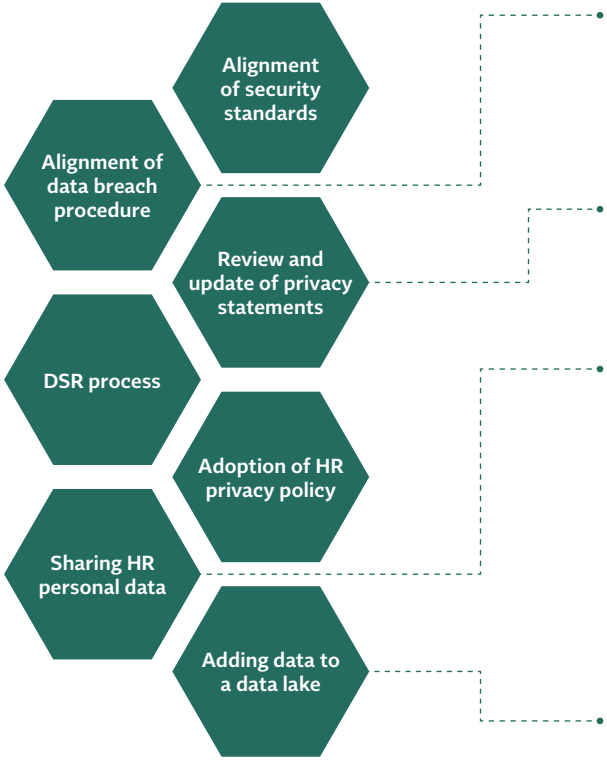
Adoption of the data privacy governance policy

Our data privacy governance document is the basic document setting out key principles of data processing to which an organization adheres. It is recommended to adopt the document by the target as soon as possible.

Privacy and security awareness trainings

Take into the account the nature of the business and language used for day-to-day operations. It may, for example, turn out that some additional aspects of processing data need to be emphasized or that a local language version of a privacy training is needed.

Integration



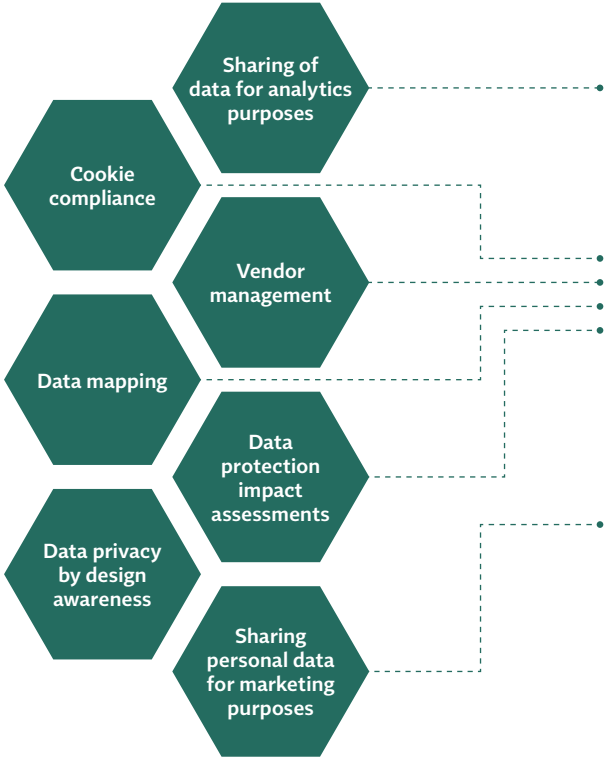
- Some businesses — in particular, those from jurisdictions that do not have modern data protection laws — may leave privacy out of incident management processes. Aim to update the procedures so that the privacy lead is part of the incident assessment and response planning and that any statutory notification deadlines are met, such as 72-hour deadline for incidents affecting EU individuals' personal data.
- Depending on the maturity of the business and level of integration, you may want to align the privacy statements with the acquiring business's template or only make necessary adjustments. Remember to update any references to the group of companies to which the target pertains and to include information about any planned sharing and use of personal data.
- Most commonly, the HR function will require the target employees' data to be shared for people management purposes.

Intragroup contract › **Evaluation of local legal requirements** › **Communication to employees/obtaining employee consent** › **Transfer of HR personal data**

The transfer of data will require prior adoption of a contract and evaluation of local legal requirements. Usually, a notice to employees should be sufficient, but in certain jurisdictions, specific consent may be required (e.g., Indonesia). Remember that no more data should be shared than necessary to meet the purpose of sharing.

- Consider any data transfer restrictions and localization requirements and appropriate customer disclosures when changing the location of the target's data.

Integration



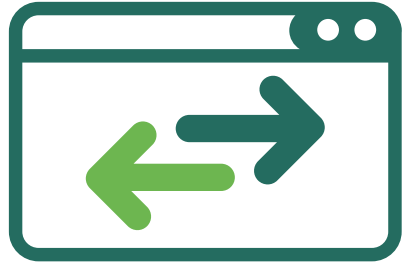
After the transaction, the business intelligence teams may intend to use the target's data for group analytics. Make sure to assess the feasibility of such use of data, taking into the account any required customer consents and notifications, and introduce appropriate controls and security measures for that purpose.

Some companies likely already have dedicated tools to ensure compliance in those areas that could also be used by the acquired target businesses. Note that onboarding of the target to a purchaser's systems usually requires significant involvement on the purchaser's side, which should be taken into consideration from the privacy team's capacity perspective.

Using the target users' personal data for other or extended purposes than collected prior to acquisition — for example, for marketing of other businesses' products — usually requires a separate opt-in consent from each of the users. Often business stakeholders plan to use personal data of a target in such manner — be watchful and educate business stakeholders on such limitations.

2. Acquisitions and divestments

Transaction preparations — General privacy considerations



The seller's engagement with the potential buyer is preceded with preparations for the transaction, including such activities as valuation of the target business and setting up the data room. Depending on the size of the target, this period may take even several months. In relation to such preparatory activities, certain privacy principles should be observed. Please see the guidelines below for details.

General rules on personal data protection in documents revealed to the potential buyer

- Use pseudonymized or, ideally, anonymized data, for example, in an aggregated form. If any personal data needs to be disclosed in relation to specific individuals, limit such data as much as possible and document the reasons for disclosure.
- Avoid disclosing such data as, for example, information on racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, and health data.
- If personal data of sensitive nature need to be disclosed (e.g., management contracts), consider using additional security measures, such as clean teams.
- In case of doubts related to disclosures, reach out to the privacy counsel.

Data room setup

A majority of divestment transactions will require setting up a data room. Whether you are a transaction team lawyer or an in-house lawyer brought over the wall, you may need to indicate how the data room should be set up and what documents should be revealed to the potential buyer to allow it to assess privacy risks of the divested business. In addition, to the general rules set out on the previous page, please find some suggestions below.

Agreement with the data room provider and data room setup

The data room provider hosts data located in the due diligence documentation, as well as user data; therefore, it acts as a data processor.

- Make sure the agreement with the data room provider include appropriate data processor clauses, including clauses addressing any international data transfer restrictions, if applicable.
- Consider disabling document copying, saving and printing.
- Make sure the persons accessing the data room accept a confidentiality undertaking.

Privacy documents to be shown in the data room

The scope of data depends on how detailed the due diligence is planned to be. Below please find several considerations when preparing a seller's data room:

- Privacy statements.
- Data-mapping records — Double-check whether they do not reveal information that is considered confidential in other parts of the data room (for example, names of vendors and partners).
- Data processing agreements — Consider uploading templates rather than copies of the actual DPAs.
- Policies — Be mindful that policies used for the entire group may reveal certain confidential information about the seller's business that is not divested; in such case, consider redacting relevant parts of the policy.
- Information about data breaches, legal proceedings and notification to data protection authorities — Consider limiting those to a specific time period, e.g., three years preceding the transaction; align this with other legal proceedings documentations.
- If new laws are to be implemented in the target's jurisdiction, consider showing an overview of the planned steps for compliance with new laws.
- An additional note or memorandum may be useful to give a better feel of maturity of the privacy program.
- Other information that may be worth showing in the data room include information on compliance with industry standards (e.g., payment card industry) and on security and privacy audits.

VDD and other privacy support in transaction

Divestment transactions may require involvement of an in-house privacy counsel at various stages. On the previous page, you could find general guidelines related to preparation of the transaction. Here you will find a close-up of the most common phases of a sale transaction where privacy input may be needed.

Vendor due diligence

Before a transaction, the buyer may choose to commission an external advisor a VDD to show the potential buyer an independent analysis of legal, financial and other aspects of the target business. A privacy counsel may be brought over the wall to support the advisor in preparing the VDD report. Keep in mind that:

- VDD reports are usually descriptive (unlike DD reports prepared for buyers, which are usually red-flag reports) and do not contain recommendations on further actions.
- VDD reviews allow identification of gaps to address and eliminate before the transaction.
- VDD reports can be used to deliver an overview of the privacy program and additional context to the documents that buyer will find in the data room.

SPA negotiations

As you may read in detail in the chapter on acquisitions, upon identifying privacy risk, the buyer may want to impose specific obligations or liability provision on the seller. The transaction team may elect to consult the in-house privacy lawyer with respect to relevance of such additional provisions. Please see pages 16 and 17 to learn more about risks and SPA undertakings.

Disclosure schedule

Another document that an in-house privacy counsel may need to contribute to is a disclosure schedule. As described on page 17, the buyer may request certain representation and warranties from the seller to confirm certain facts. A disclosure schedule is aimed to reveal exceptions to representations and warranties given by the seller (e.g., if a warranty states there have been no data breaches discovered within the past three years and, in fact, there has been one, then it should be disclosed in a disclosure schedule). Disclosure schedule is usually prepared at the end of the SPA negotiations when the scope of representations and warranties is agreed.

Separation and migration

Like integration projects, separation projects can be simple and require little effort on the seller's side if the target business is standalone. However, in the case of businesses highly integrated with the seller, they can prove to be challenging and involve months of detailed operational work to migrate data to new systems that are to be used by the target.

Some of the general comments made in this playbook in relation to a TSA (page 18) and completion (page 19) can apply to the separation process and accordingly will not be repeated here. However, below you can find some additional tips on what to look at when approaching the separation and migration process.

Remember that frequently, system architecture and controls are not designed with a potential separation in mind. It is worth assessing as early as possible what systems are used for processing personal data related to the target business, and — if those systems are shared with the seller — checking whether the target's data can be easily separated from the seller's other data in case of migration to the target's or the purchaser's environment. This can help to appropriately shape the TSA provisions and/or the migration plan.

Consider whether a copy of any data relating to the divested business needs to be retained by the seller or its group. The reasons for such data retention may include, for example, financial reporting obligations or legal claims. The scope of retained data will largely depend on the structure of the transaction (e.g., in the case of an asset transaction, the seller is likely to keep more data than in the case of a share transaction). At all times, remember to assess whether the seller has a sufficient legal basis for retention of such data.

In certain situations, the seller may need a separate legal basis, such as consent, for transfer of personal data to the purchaser (e.g., in the context of an asset transaction). From a general privacy perspective, it is of utmost importance that in the case of transfer of assets from one company to another the transfer of data is conducted in a transparent manner and that users/data subjects have an easy, executable choice, should such choice be relevant and necessary.

3. Liquidations

Liquidation — Basic information

A liquidation process is aimed at bringing the business of a company to an end and closing the company. It may happen, in particular, if a company's business has been transferred to another entity as a result of an asset transaction; it may also happen that the entire company's business is closed. Liquidation process is governed by the laws of the liquidated company's incorporation; however, there are some similarities in the stages of the process across various jurisdictions, which have been outlined below.

This stage involves closure of a business. This stage make take months or even years. The liquidated company is obliged to comply with its data protection law obligations.

The liquidated company ceases to exist. Any personal data that needs to be retained is handed over to an entity appointed to keep records following the liquidation.

Opening of liquidation → **Liquidation of assets and adjudication of claims** → **Distribution of liquidation proceeds** → **Dissolution of a company** → **Record keeping**

Opening of liquidation can be voluntary (usually on the basis of a shareholders' resolution) or ordered by a court.

This stage directly precedes the dissolution of the liquidated company. Any assets left after closure of the business may be distributed to the company's shareholders.

The entity appointed to keep the records administers the retained personal data until the end of the retention period.

Liquidation — Privacy aspects

Although liquidation of a company is aimed at ending a company's business, privacy laws apply to the company until it is finally dissolved. Therefore, the company should maintain at least minimum privacy compliance and take privacy requirements into account when concluding its business.

Processing personal data after opening of liquidation

As mentioned on the previous page, the liquidated company needs to comply with its legal obligations in the same way as before opening of the liquidation. In particular, it is obliged to appropriately secure data, keep its data-mapping records, maintain a DPO position if required by law, and respond to DSR requests. Be prepared that upon public announcement and/or communication about the opening of liquidation, there may be a significant increase in the number of DSR requests, particularly requests for data erasure.

Retention of personal data

Consider what personal data related with the closed business will need to be retained following liquidation. Usually, such data retention is either required by law (e.g., employee data) or needed for the purposes of authorities' audits (tax data). Retention of personal data for other purposes (analytics, marketing) after the liquidation of a company being a data controller would most likely require separate consent of data subjects.

Communication to individuals

At a certain point of the liquidation, you will need to communicate to customers what will happen to their personal data after the liquidation and provide them with contact details for DSR requests. You should be able to provide updates to the notification after the business is liquidated to reflect any changes that may relate to the data.

Administration of personal data after company dissolution

Local laws usually determine who may hold liquidated company's records — for example, whether this needs to be a governmental entity or another company. The entity keeping the retained personal data will need to ensure the retained data is kept in a secure manner (in particular that it is encrypted) and that it can only be accessed when required under law. Moreover, the entity will need to respond to DSR requests and reflect the kept personal data in its data-mapping inventory.


iapp
prosus