Johnson Hana.

Replacement Standard Contractual Clauses (SCCs)

A Practical Guide

July 2021

A detailed guide to the new Standard Contractual Clauses and how organisations can achieve compliance.

Table of Contents

Part one

Guide to the New SCCs.

Introduction to Part One

On 4 June 2021, the European Commission ("EC") adopted new standard contractual clauses ("New SCCs") for transfers of personal data to a third country which are governed by the General Data Protection Regulation 2016/679 ("GDPR").

Part 1 of this Whitepaper provides background on how and why the New SCCs were introduced and considers the implications of their introduction.

Part 2 sets out a detailed practical implementation guide, providing a framework for organisations to understand what they need to do to achieve compliance.

Background to SCCs

Keeping up with a changing world

Data controllers and processors that are subject to GDPR can only, under Chapter V of the legislation, transfer personal data to a third country outside the EU/ European Economic Area (EEA), if:

- an adequacy decision exists in relation to that country, i.e., the EC has issued a decision confirming that that country's data protection standards are broadly equivalent to the EU;
- an appropriate safeguarding mechanism is used, such as standard contractual clauses or binding corporate rules, which ensure that EU standards of personal data protection "travel with the data"; or
- a suitable derogation exists which covers the circumstances of the transfer.

The previous standard contractual clauses ("Old SCCs") were introduced under Directive 95/46/EC (the "Data Protection Directive"), with the goal of ensuring appropriate data protection safeguards for transfers to third countries. The Old SCCs were approved for inclusion in contracts by the EC as an appropriate safeguard for European personal data transferred overseas. The Old SCCs were issued in 2001, with updates in 2004 and 2010.

The various forms of standard contractual clauses are considered to be "appropriate safeguards" (making up for local laws that may otherwise be deemed to be inadequate by the EC) because (i) they impose non-EEA organisations with contractual data protection obligations; and (ii) they contain a third party beneficiary clause, whereby data subjects can sue these non-EEA organisations in a European court for breach of contract if they fail to abide by the contractual data protection obligations.

It is difficult to overstate the seismic change the world has undergone since the introduction of the Data Protection Directive in the 1990s. As Advocate General Jääskinen commented, at the time the directive was written, "nobody could foresee how profoundly [the internet] would revolutionise the world". It was these technological advances among others that brought about the need for a new regime of data protection. This came to us in the form of the GDPR. Without any update to the Old SCCs following introduction of the GDPR however, for the last number of years organisations have had to rely on a set of standard contractual clauses that predated and did not contemplate the GDPR.

Background to Schrems II

Who is Maximillian Schrems?

KEY TAKEAWAY 1

Companies must ensure that EU persons' data held outside of the EU remains compliant with GDPR.

Maximillian Schrems is an Austrian privacy activist who has brought multiple claims against American technology companies to the courts. Last year he had a significant victory in the European Courts in the "Schrems II" case . Schrems was concerned by Facebook's transfers of data from the European Union to the United States; in particular, he was worried about the access the United States National Security Agency ("NSA") would have to the data of Facebook's European users through the NSA's PRISM mass surveillance programme.

The particular transfer mechanism that he sought to challenge, in order to halt the data transfer, was the Privacy Shield, on which many transfers to the United States relied. The Privacy Shield was an agreement between the EC and the United States allowing for European personal data to be transferred from the EU to the United States, provided that the importer made a public declaration that they would follow specific standards. This was enforceable under US law. However, US law still allowed for the interception of European data by American intelligence agencies. For this reason, in the Schrems II case, the Court of Justice of the European Union ("CJEU") held that US law did not meet the four European Essential Guarantees and invalidated the Privacy Shield, effectively halting most transatlantic data transfers. The CJEU did however uphold the validity of the standard contractual clauses.

KEY TAKEAWAY 2

There is no adequacy decision for the US, so, in the absence of a suitable derogation, SCCs and binding corporate rules are the only options for a transfer mechnism.

As a result of the Schrems II decision, many data exporters sending personal data to the US had to cease relying on the Privacy Shield and only transfer personal data by using the standard contractual clauses. Given the materiality and volume of transfers to the United States, (and as there is no adequacy decision in respect of the United States), the standard contractual clauses became significantly more important as the principal mechanism to transfer personal data from the EEA to the US.

Note that although the CJEU upheld the Old SCCs as a valid transfer mechanism, the court stressed that organisations must, on a case-by-case basis, verify that EU personal data being transferred outside of the EU would be adequately protected in the destination country in line with the level of protection set out in the GDPR.

The New SCCs

Consequences of Schrems II

The Schrems II decision spurred the EC into action to update the now outdated Old SCCs and the EC issued a draft implementing decision on standard contractual clauses on November 12 2020. The final text of the New SCCs was issued on 4 June 2021 and published in the official journal on 7 June 2021, becoming effective on 27 June 2021. The New SCCs will repeal and replace the Old SCCs and address the entry into force of the GDPR and the decision of the CJEU in Schrems II. The New SCCs enhance the protection for data subjects in comparison to the Old SCCs and attempt to solve the issues arising from the implementation of the GDPR and the Schrems II decision since the adoption of the last version of the Old SCCs.

GDPR Update

The New SCCs have been updated generally to bring them in line with the current GDPR standard of data protection, as opposed to the Data Protection Directive, bringing certainty in several areas where previously there were gaps or inconsistencies. In particular, the New SCCs include new and significant obligations for data importers, particularly importers acting as controllers, reflecting GDPR requirements. The New SCCs also include processor terms as required under Article 28 of the GDPR, addressing a gap in the Old SCCs, which were drafted long before the GDPR requirements for minimum processor terms came into force.

Many obligations arising under the Old SCCs will continue to apply, for example, the obligation on the exporter to consider the extent of protection for personal data in the third country already exists under the Old SCCs. Similarly, third-party beneficiaries' rights continue to be enforceable against both the exporter and the importer. The basic processor / controller obligations under EU law have also been clarified; in controller to processor and processor to processor scenarios, the new Article 28 requirements have been included.

In general, the New SCCs bring some much-needed clarity to the steps required to transfer personal data to third countries, including the factors to be assessed by data exporters and data importers, as well as on the measures that can be taken to ensure that protection equivalent to that afforded to personal data in the EU is assured in the importing country. The obligations on both data exporters and data importers to comply with the clauses remain onerous, however.

KEY TAKEAWAY 1

The new SCCs are now aligned with the GDPR as opposed to the Data Protection Directive.

KEY TAKEAWAY 2

The updated requirements for data transfers in the New SCCs reflect the judgment of the CJEU in the Schrems II case.

Key Changes in the New SCCs

There are some key changes in the New SCCs that organisations should be aware of, ranging from how the clauses are structured to specific new requirements and obligations imposed on importers and exporters. In this section we highlight those changes and provide context for organisations to understand what they will mean for their compliance.

Modular approach

The New SCCs have been constructed in a modular manner whereby different clauses are available depending on the relationship involved. Rather than having different sets of clauses for the various permutations of relationship between exporters and importers, the New SCCs provide for one set of clauses only, with different modules to be used as appropriate to the relationship in question. Module one covers controller to controller relationships; module two covers controller to processor relationships; module three covers processor to processor relationships; and module four covers processor to controller relationships. These four modules better reflect the various types of international transfers of data than the Old SCCs did, which did not cover processor to processor or processor to controller data transfers.

Flexibility

As mentioned above, the modular approach taken in the New SCCs allows greater flexibility with respect to the different types of relationship that may apply to data transfers. The New SCCs also provide more flexibility on the jurisdiction of the importer and exporter – the Old SCCs required the data exporter to be established in the EEA. If the data exporter was not based in an EEA country, the standard contractual clauses were not available as a valid data transfer mechanism. This issue has been resolved in the New SCCs, which can be used for transferring personal data from one party not based in the EEA to another party also not based in the EEA, for example from a processor to a sub-processor. The New SCCs also provide further flexibility around governing law and jurisdiction, allowing the parties the option to choose the governing law of any Member State to apply to the contract.

Note, for data transfers between controllers and processors, the New SCCs include the requirements set out in Article 28 of the GDPR (for agreements between controllers and processors), which means that the parties to such data transfer agreements will not need to complete a separate Article-28 style data processing agreement.

Increased scrutiny of assessment of third-party security

The consequence of the Schrems II decision is an increased scrutiny of the laws and security of the third-party country and importer to which data will be transferred. This is represented in the New SCCs thanks to a new mutual warranty, which forms an essential part of each module of the clauses. The warranty requires all parties to declare that they have no reason to believe that the laws and practices of the third country would prevent the data importer from fulfilling its obligations under the New SCCs, including its obligations to keep the data safe and comply with data subjects' rights. This warranty underpins the transfer impact assessment which data exporters, together with their importers, will have to complete when contemplating transferring data to third countries using the New SCCs as their transfer mechanism. The requirement for the transfer impact assessment was also highlighted in Schrems II and in the substitute guidance issued by the European Data Protection Board ("EDPB").

The New SCCs also clarify the factors that a data exporter and importer must consider in order to provide the warranty, including the specifics of the data transfer, the laws and practices of the destination country (in particular any laws requiring disclosure of data to public authorities), and any relevant contractual, technical or organisational safeguards put in place to supplement the New SCCs. This assessment must be documented in a formal data transfer impact assessment, which must also be available to regulators upon request.

To the best of its ability, an Importer must warrant that it has provided relevant information and ongoing cooperation. There has also been an expansion of the right of supervision and termination where an exporter has reason to believe that an importer is unable to comply.

Key Changes in the New SCCs

Increased notification obligations

The New SCCs provide for new measures to deal with attempts by authorities to access transferred data. In the case of attempt by a public authority to access the data, the New SCCs require the data importer to:

- immediately notify the data exporter on receiving a legally binding request for disclosure from a public authority, or on becoming aware of a public authority gaining direct access to the relevant data;
- use best efforts to obtain a waiver from the public authority if local laws prohibit the data importer from notifying the data exporter as required above; and
- report the requests regularly to the data exporter, keep records, preserve all documents, assess the legality of the request and, where there are reasonable grounds to do so, challenge such requests. If this is not possible, the importer must only provide the minimum amount of information possible to the public authority. The data importer must also document its legal assessment of any such access requests and make this available to the data exporter and/or competent supervisory authority upon request.

The New SCCs introduce an obligation of transparency for the data importer which goes over and above the regular audit reports demonstrating compliance with the requirements of the Old SCCs. The data importer should regularly provide the data exporter with the greatest amount of relevant information on any governmental requests for disclosing personal data transferred. Such transparency reports should include information around the number of requests received, type of data requested, the requesting authority, whether the request has been challenged, and the outcome of the exercise.

There are also enhanced transparency obligations on parties with respect to information to be made available to data subjects, which must include the identity and contact details of the importer, the categories of personal data processed, and details of any onward transfer(s). Importers are also required to notify data subjects if a public authority requests access to a subject's data. The requirement to notify data subjects exists under all modules of the New SCCs. Finally, the text of the New SCCs executed between the data exporter and importer should be made available on request to data subjects as well, although confidential information (for example, detailed technical measures that the parties do not wish to disclose) can be redacted.

Requirements for data importers

The New SCCs impose significant obligations on non-EEA controllers and processors, notably in terms of information to be provided to data subjects, as detailed above. They also require the data importer to assess and declare that the laws and practices in the third country of destination, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent the data importer from fulfilling its obligations under the SCCs. For data importers not already subject to the GDPR (through its extraterritorial effect), this will likely require them to adopt a significant compliance program with respect to data protection, including policies, procedures and dedicated resources as required. It is also essential for importers to keep the transfers under constant review as the situation in the third country will not be static.

Liability allocation and docking clause

The New SCCs provide for allocation of liability between the parties. Each party is liable to the other for the damage resulting from its breach of the New SCCs and each party is also liable to the data subject for any damage it causes. For controller to processor and processor to processor transfers, the exporter is also liable to the data subject for the damage caused by either party. The New SCCs also contain a contribution clause stating that if the parties are held jointly and severally liable for a breach of the New SCCs, they are entitled to assert a claim against the other party for compensation corresponding to its/their responsibility for the damage.

Finally, reflecting widespread practice in the market, the New SCCs facilitate multi-party use, and include an optional "docking" clause. These provisions allow additional controllers and processors to accede to the clauses throughout the term, provided that the original parties to the clauses opted to include the docking clause. These provisions can apply even after the initial signing of the contract allowing for additional flexibility.

Complications

Although in general the New SCCs introduce greater flexibility for the various types of importer/exporter relationships, and bring some welcome clarity to certain types of transfer arrangements, nevertheless there are some complications in their application. In particular, three principal issues have been identified, (i) how the New SCCs will apply to transfers involving the UK in a post-Brexit world, (ii) how data subject rights can be enforced in the context of privity of contract rules in Ireland, and (iii) use of the SCCs where the data importer is already subject to GDPR.

Application in the UK

One of the consequences of Brexit is a significant likelihood of misalignment in data protection standards and requirements between the UK and the EU. The UK government has been attempting to remedy this to some extent by transposing European laws into UK law, including through the United Kingdom General Data Protection Regulation ("UK GDPR"), which was an amendment of the UK's Data Protection Act brought about by the UK's European Union (withdrawal) Act 2018. UK GDPR is almost identical to the GDPR, except that the cooperation mechanisms and ability to make delegated acts have been removed (Chapters VII and X).

The potentially significant impact of regulatory dealignment can be seen through the introduction of the New SCCs by the EC. UK GDPR only makes reference to the Old SCCs, and due to this dealignment, it is not yet clear if the new ones will be recognised. The UK Information Commissioner's Office ("ICO") is expected to issue its own standard contractual clauses, which it is anticipated will be similar to the New SCCs, offering increased protection. The ICO is currently in the process of updating its advice on use of standard contractual clauses. In the meantime, the New SCCs will not apply to transfers of personal data from organisations which are subject to UK GDPR. In these circumstances, and until the ICO has confirmed otherwise, a UK data exporter should continue to use the Old SCCs in respect of its data transfers to third countries.

Note on 28 June 2021, the EC approved the UK's data protection standards as being sufficient to receive an adequacy decision; meaning that the EC considers the UK's data protection regime to be essentially equivalent to the EU. The UK will join a select list of non-EEA 'third countries' to which EU-regulated personal data can continue to flow without further restrictions or another transfer mechanism like the New SCCs. Other countries on this list include Argentina, Israel, New Zealand, Switzerland, and Japan. In a reciprocal move, the UK has also confirmed that UK personal data can continue to be transferred to the EEA as previously.

The adequacy decision is reviewed every four years and so data importers and exporters should be aware that they will need to continue to monitor the position with respect to transfers involving UK entities.

Irish privity of contract

As mentioned above, the modular approach taken in the New SCCs allows greater flexibility with respect to the different types of relationship that may apply to data transfers. The New SCCs also provide more flexibility on the jurisdiction of the importer and exporter – the Old SCCs required the data exporter to be established in the EEA. If the data exporter was not based in an EEA country, the standard contractual clauses were not available as a valid data transfer mechanism. This issue has been resolved in the New SCCs, which can be used for transferring personal data from one party not based in the EEA to another party also not based in the EEA, for example from a processor to a sub-processor. The New SCCs also provide further flexibility around governing law and jurisdiction, allowing the parties the option to choose the governing law of any Member State to apply to the contract.

Note, for data transfers between controllers and processors, the New SCCs include the requirements set out in Article 28 GDPR (for agreements between controllers and processors), which means that the parties to such data transfer agreements will not need to complete a separate Article 28 style data processing agreement.

Application where the importer is already subject to GDPR

It is possible for a data importer established outside the EEA to already be subject to the GDPR through its extraterritorial effect, however it is not currently clear if the New SCCs can be used for transfers to such importers as the clauses only contemplate transfers to importers who are not presently subject to the GDPR. It is likely that guidance will be required from the EDPB to bring clarity on this point.

Part two

Practical Implementation Guide.

Introduction to Part Two

Much has been written about the New SCCs, Schrems II and the legal requirements arising for importers and exporters. Organisations may well be left wondering how they are actually going to tackle a project of this scale however. To do so, they will need to understand in detail the steps required to achieve compliance, and preferably how to operationalise that compliance for new transfer arrangements going forward.

In this Part 2, we have set out a detailed framework for compliance with the New SCCs, scoping out the practical steps that organisations should take and the timelines they need to be aware of in doing so. This breaks down into 3 key phases or mini-projects, data mapping, transfer impact assessments and the repapering exercise (including policy and compliance program updates). Each of these is considered in detail in the following pages.

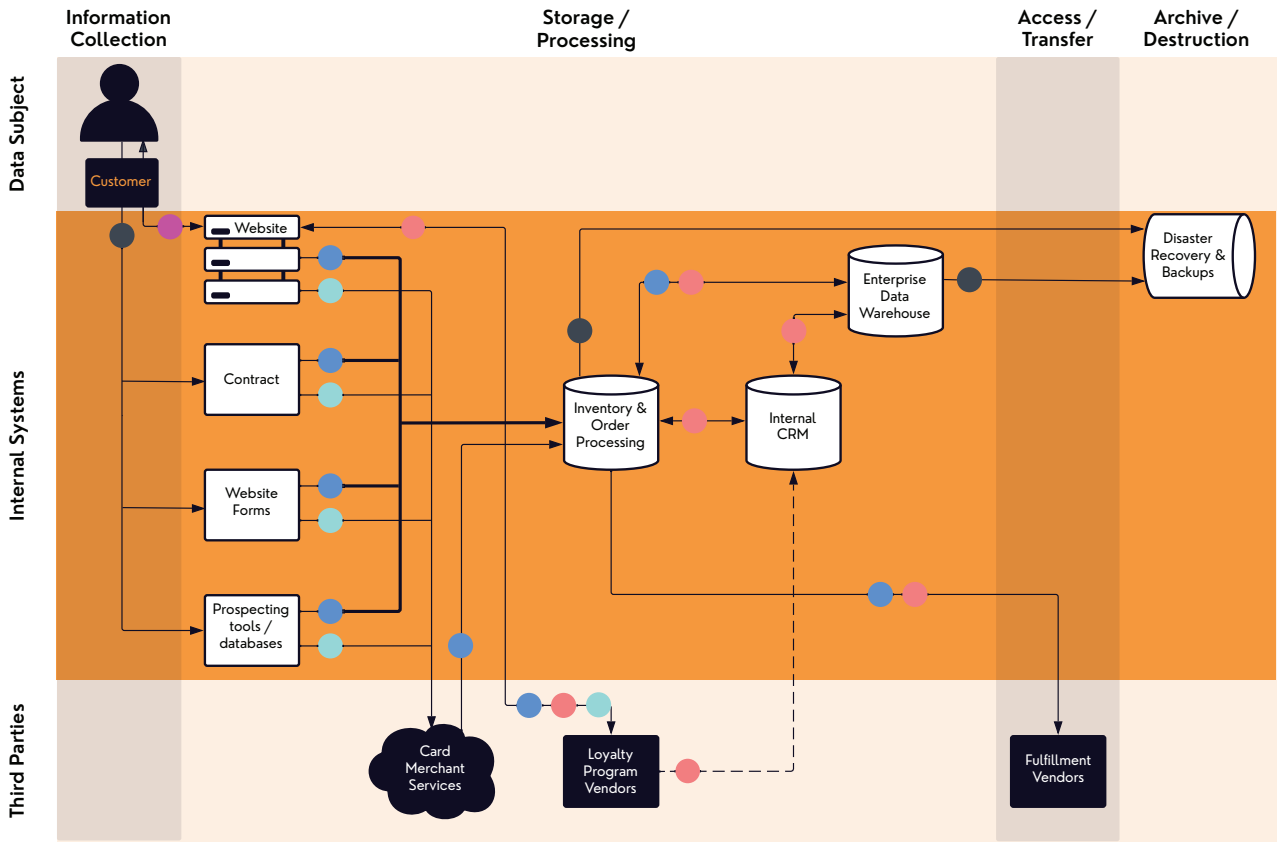
Data Mapping

The first step to achieve compliance with the requirements of the New SCCs is to map out an organisation's data and data flows.

This is a crucial part of the process as organisations will need to have a deep understanding of where their data is, what transfers it undergoes, to whom, and for what purpose, before they can effectively comply with their obligations arising under the New SCCs.

Below you can see an illustration demonstrating how data flows through a company and related third parties:

Sample Data Flow Map



Legend

- Combined Data: Personal Data, Transactions, Financial Data, Web Session Data.
- Cookies, Behavioral Tracking, Unique Identifiers
- Financial Data (sensitive); Credit Card Transaction Elements
- Transaction Data: Purchase Record, Confirmation Number, Invoice Number, Shipping/ Tracking Numver, etc.
- Customer Data (non-sensitive): Email, Phone, Address, etc.

How to build a data map

What personal data does your organisation hold?

- If you already have a personal data inventory, you should carry out an audit to ensure that it is up to date, and that you have a good understanding of the nature of the personal data that you hold, where and how it is stored and the categories of data subjects to which it relates.
- Remember, personal data means all information that relates to an identified or identifiable individual. This could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier.
- If you do not have a personal data inventory, or your inventory is out of date, you will need to create one. Generally, you have two options for doing so, manually or using a technology tool.
    - The first option is to conduct a manual information search. You should nominate a responsible person from each business unit within your organisation to identify what personal data their unit accesses, holds or uses. This is typically done through questionnaires and informational interviews. The data is usually gathered via in-person or paper surveys before being collected and analysed.
    - In organisations with complex data, it may be worth using software to engage in a technology assisted search to gather the necessary information. Typically, this is gathered through electronic questionnaires that are filled in online or via scanners that detect data collection and its movement around the electronic systems of the organisation.
    - Johnson Hana provides legal and privacy technologies and can work with your organisation to identify a suitable technology solution if appropriate.
    - Assuming implemented correctly, both options should result in the same output, i.e., a detailed description of the personal data held by the organisation.
- Note, personal data can reside in multiple locations and can be stored in many formats, such as paper, electronic and audio. It is important that the audit of data held is as thorough as possible to ensure that you know exactly what personal data is involved.

How to build a data map

Who are the data subjects?

- Once you have identified what personal data your organisation holds, the next step is to identify all relevant categories of data subjects. Data subjects are natural persons about whom personal data is held and who can be identified directly or indirectly from that personal data.
- Based on your mapping of the data held by your organisation in the previous step, you should be able to identify the categories of individuals in respect of whom you hold personal data.
- The anticipated categories will vary significantly based on an organisation's operational set up, business model and industry. As a guide however, you should be considering employees, contractors, customers, prospects, suppliers, users of your website and other individuals targeted with cookies or other tracking technologies.

Where is the data stored and how does it flow through the organisation?

- As part of the data mapping exercise, you should identify where in the organisation any personal data is held, and in what format.
- From there, ascertain all entry and exit points for the personal data, along with any interim transfers. Organisations need to know where their data is going, both internally within the organisation and externally to and from third parties. Where does the data come from, how is it collected, where does it go and how?
- Mapped data flows should state whether the data crosses borders for each data flow. Note this is required even when it is being moved for internal purposes only, not involving a third party.
- Remember that remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EU/EEA, is also considered to be a transfer.
- At the end of this step, you should be able to identify how personal data enters the organisation, where it is collected from, where it ends up, and each place that it stops along the way. This may be via different systems, tools and/or legal entities.

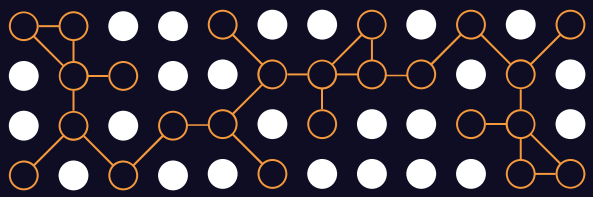
How to build a data map

Identify counterparties and relationships

- With the data flows mapped out, you should be able to identify who the counterparty in each data flow is. This may be other group entities, or it may be third parties, including your technology providers, suppliers, subcontractors, government agencies, customers etc.
- For each counterparty, you should determine in what capacity each of you is acting with respect to the personal data in question, i.e., as a data controller or data processor? Having this element of the data mapping done will be crucial to understanding which module of the New SCCs is required for existing transfers.
- At the outcome, you should have the specific counterparty for each flow of personal data as well as the capacity in which each party to the data flow acts.

Where are the relevant contracts?

- Lastly for your data mapping exercise, you will need to identify and locate any contractual arrangements applicable to each data flow. Is there a contract in place and if so, where is it? Who has access to those contracts? Are there any contracts missing? Application of a contract management system in this instance can be very useful as all of your contracts will be stored in one location and contractual information will be instantly accessible. With summaries for each contract, it will be quicker to identify key regulations or terms and identify any missing information. Additionally, using a contract management system enables organisations to monitor access to contracts and automatically control permissions.
- This step is crucial in setting you up for the repapering exercise required to implement the New SCCs.



Transfer impact assessments

The obligations on organisations to risk assess all relevant third country data flows to which they are party is one of the key elements of adoption of the New SCCs. As noted above, parties are required to warrant in the New SCCs that:

> *"they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses".*

In order to understand their risk in giving this warranty, parties need to conduct an assessment of the transfer risk and impact based on the laws and regulations of the country to which the data is being transferred. This assessment must be available to supervisory authorities if requested and accordingly must be documented and up to date.

The New SCCs identify specific elements that parties must take into account in doing so, including:

- *"the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred"*;
- the laws of the data importer and applicable limitations and safeguards; and
- safeguards like technical and organisational measures applied during transmission and to the processing of personal data in the country of destination.

In a footnote to the above text of the New SCCs, some further guidance on the factors for consideration is provided:

> *"Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests".*

According to the EC guidance, organisations seeking to rely on such factors must ensure that any *"practical experience"* relied upon covers a sufficiently representative timeframe; that other relevant, *"objective"* elements support the practical experience; and that other information, case law, or independent reports corroborate and do not contradict the practical experience.

Note if the assessment fails to confirm at least equivalent levels of protection, or the level of protection drops because of legislative or other changes, the data exporter has an obligation to suspend the transfer immediately and the right to terminate the contract.

Transfer impact assessments

Organisations should consider the following steps to comply with the requirements of the New SCCs and carry out suitable transfer impact assessments for their data flows:

Categorise data flows

The relevant third country data flows identified in the data mapping exercise should be audited, categorised and prioritised depending on the nature of the arrangement and the counterparty, how important the data transfer is to a business, the destination countries that a business exports data to, and the type and amount of data which is being transferred.

Prepare a template assessment document

Organisations should work with their advisors to develop a template for conducting transfer impact assessments. The elements of the assessment will vary depending on the nature and sensitivity of the data being transferred and the third-party jurisdictions involved. However, organisations should consider the following general areas for the assessment:

Details of the data involved:

- Exactly what personal data will be transferred? Is any of it classified as sensitive?
- Who are the data subjects involved?
- For what purpose is the data to be transferred?
- Types of entities involved in the processing (public/private; controller/processor).
- Sector in which the transfer occurs.
- Will the data be stored in the third country or is there only remote access to data stored within the EU/EEA?

Transfer details:

- Mechanisms / tools used for the transfer.
- Current technical / organisational measures applied.
- Format of the data to be transferred (i.e., in plain text/ pseudonymised or encrypted).
- Possibility that the data may be subject to onward transfers by the importer to another third country.
- The relevant legal basis (e.g., adequacy decision, Article 49, SCCs, etc).

Transfer impact assessments

Prepare a template assessment document (continued)

Assessment of third country legislative framework:

- The exporter and the relevant importer must carry out a case-by-case analysis to check if there are any national laws to which the importer is subject that violate the GDPR and the Charter of Fundamental Rights.
- Accordingly, the template assessment should require details of:
  - the applicable third country legislative framework;
  - possibility of governmental surveillance;
  - previous or potential cooperation with governmental authorities;
  - ability to refuse requests for access to data by authorities; and
  - any other laws to which the importer is subject that could give rise to an obligation to disclose data.
- Note, generally laws that allow enforcement access to data in individualised cases and subject to the approval of a judge will be compliant with EU law. Forms of less democratic, far-reaching access (mass processing) or access without judicial review are generally not in line with EU law.
- Are the four European Essential Guarantees respected in the relevant third country where the data are sent? These are:
  - processing should be based on clear, precise and accessible rules;
  - necessity and proportionality with regard to the legitimate objectives pursued must be demonstrated;
  - an independent oversight mechanism should exist; and
  - effective remedies need to be available to the individual.

Supplementary measures:

- Identify any supplementary measures to be applied to manage any risk identified in the assessment. For example:
  - technical measures like encryption, pseudonymisation and split processing;
  - contractual measures like obligations to implement specific technical measures and specified transparency obligations on the data importer; and
  - organisational measures like Internal policies and regulations for the transfer of data, a procedure for documenting requests from and responses to public authorities and publishing transparency reports, strict data access and confidentiality policies and adoption of standards and best practice, such as data security and privacy policies based on EU certification or codes of conduct.

Final assessment / decision:

- The template should document the organisation's assessment of the third countries' surveillance laws against the European Essential Guarantees (detailed above), as mitigated by any technical measures implemented (or through further contractual or organisational measures).
- Note, if the organisation concludes that the third country poses a risk of excess surveillance not sufficiently remedied through supplementary measures, the transfer should not be initiated or, if already in place, should be halted immediately.

Transfer impact assessments

Implementation of Procedures / Processes

Establish a process for conducting transfer impact assessments (TIAs) as follows:

- to the extent not completed previously, all existing data transfers should be assessed as soon as possible – if there are a number to be completed, these should be prioritised in accordance with their importance / sensitivity (as discussed above);
- implement a regular cadence to audit ongoing transfers previously assessed and confirm ongoing effectiveness of any supplementary measures applied; and
- as a requirement prior to entering into any new transfer arrangement.

Exporters should ensure that their procedures facilitate carrying out the assessments in conjunction with importing parties and that there is a process in place to ensure that any follow up action arising from an assessment is undertaken. Exporters should also consider how they will assess the security of the relevant third-party countries, in particular:

- What resources do you need?
- What input from data importers?
- What is the timing?

Exporters will need to quickly establish a process (and a way of documenting it) for conducting meaningful due diligence on importers to ascertain whether they can comply with their obligations under the EU SCCs – for example, via a due diligence questionnaire backed up with supporting documentation.

KEY TAKEAWAY

Organisations should prioritise identifying their top importing countries for profiling, as well as putting the framework in place to ensure that TIAs can be carried out as required, and refreshed periodically.

Repapering

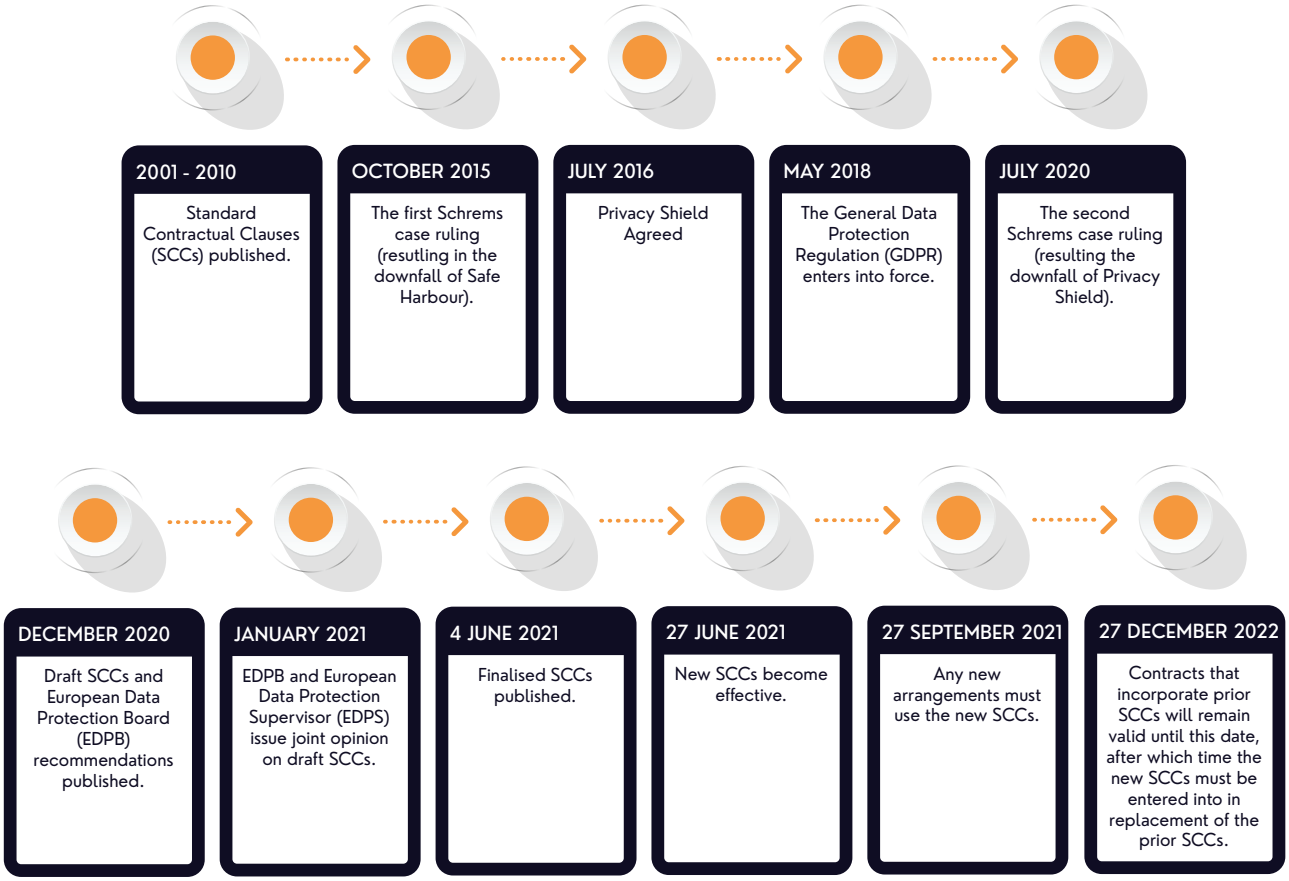
Timelines

There are two critical deadlines to keep in mind for the practical implementation of the New SCCs. The first is 27 September 2021, the second is 27 December 2022.

The New SCCs were published in the Official Journal on 7 June and took effect on 27 June 2021. Organisations can start using them from this date. The Old SCCs remain valid and effective until they are repealed on 27 September 2021 - until then, organisations are entitled to continue to use the Old SCCs for all new transfer arrangements entered into.

Organisations must cease using the Old SCCs for new data transfers with effect from 27 September 2021. From that date, the Old SCCs will no longer constitute a valid transfer mechanism.

For existing arrangements under the Old SCCs, organisations have an 18-month window, until 27 December 2022, to replace the Old SCCs with the New SCCs for those transfers. Consequently, we recommend that you implement the New SCCs as quickly as possible for all new contracts as otherwise, you are likely to have to further amend any contracts entered into between now and 27 September 2021 (unless such arrangements will terminate before 27 December 2022).



Repapering

Compliance Program & Policies

Before approaching the repapering exercise for contractual arrangements, organisations should consider other documentary updates required. For example, as detailed above, the New SCCs place extensive new obligations on exporters / importers with respect to transparency and disclosure. Depending on the nature of the transfer and relationship between the importer and exporter (e.g., controller to controller, controller to processor etc), there are obligations on parties to facilitate a data subject's right to be informed of the identity and contact details of the data exporter / data importer, the categories of personal data processed, and details of any onward transfer. The obligation can be discharged via the data exporter if the parties agree to that, and the obligation falls away if providing the information proves impossible or would involve disproportionate effort for the importer.

Organisations will need to consider how they will comply with these new requirements. Many organisations may determine that a public notice via a privacy policy or notice on a website will suffice to meet the obligations. In that case, organisations should be reviewing and amending their privacy policies to update them as required.

Note, in order to comply with the new SCCs, many importers that are not currently subject to GDPR will need to significantly update their privacy compliance programs beyond just the contract repapering exercise. This may require considerable effort for data importers, particularly those that are not otherwise directly subject to GDPR. Organisations will not only need to implement new internal policies to meet these requirements, they will also need to keep detailed records demonstrating their compliance and make these available (including for audit) pursuant to transparency requirements in the New SCCs. Organisations will need to have processes in place to actively monitor their compliance with the New SCCs across a variety of business relationships.

KEY TAKEAWAY 1

With less than 3 months remaining to the 27 September deadline, organisations should prioritise updating procedures and template documentation for new transfer arrangements.

KEY TAKEAWAY 2

For organisations that are not currently complying with GDPR but will need to enter into the New SCCs, time is short to put into place essentially a scaled down version of a GDPR compliance program.

Repapering

New Contracts

Given the short timeline to switch over to the New SCCs, organisations should be focused on implementing the changes required for new arrangements concerning transfers of personal data as quickly as possible. To avoid inconsistent or incorrect application of terms, we recommend taking a detailed project management approach to the implementation process. Using the comprehensive data map completed, organisations should begin by working with their internal and external data protection advisors to put in place a detailed playbook for application of the New SCCs to contractual arrangements. This will act both as a guide for the organisation's compliance with the implementation of the New SCCs for new transfers, and as a valuable internal resource for the contracting process.

Different organisations will have different requirements and consequently each organisation's playbook should reflect their own specific data flows, complexity and requirements. In general, however, we would recommend that the playbook cover at least the following:

Details of the different categories of transfers that the organisation is party to, i.e., any or all of:

- Controller to controller;
- Controller to processor;
- Processor to controller; and
- Processor to processor.

The playbook should clearly set out the module of the New SCCs to apply to the different category of relationships, specifying for each module:

- Any additional clauses required. Note additional clauses may be included provided that they do not contradict the terms of the New SCCs. Organisations should consider whether any additional clauses are required for each different category of relationship. For example, parties may wish to consider the following potential issues.
  - Liability allocation. Under the New SCCs, each party is liable to the other for the damage that results from its breach of the clauses. Each party is also liable to the data subject for the damage it causes, and for certain transfers, the exporter is also liable to the data subject for the damage caused by either party. It appears that it may be open to parties however to include additional clauses reallocating liability as between them provided that such allocation does not 'contradict' the New SCCs, for example by providing for a lower level of liability.
  - Insurance. Organisations should verify their own insurance coverage to ensure that they have sufficient coverage for any new potential liability relating to claims under the New SCCs. Parties may also wish to consider including mandatory insurance requirements in the clauses to ensure both parties are adequately covered.

Repapering

New Contracts (continued)

- Governing law. Parties may choose the law of any member state which allows for third party beneficiary rights. Organisations should ensure that the playbook includes their preferred governing law for each category of transfer arrangement.
- Annex details. The New SCCs include new details to be set out in the annex, meaning that organisations will not be able to just copy and paste from the Old SCCs. Organisations should consider the annex detail requirements and define particulars for each category of relationship / contract. This will include factual descriptions of the categories of data, the purposes of use, information about technical and organisational security measures, details of the supervisory authorities responsible for overseeing the data exporter, and a list of relevant sub-processors.
- Negotiation. An effective contract playbook should define the range of negotiation permitted and when escalation to more senior approvers is required. Clearly, as it is not permissible to amend the text of the New SCCs, negotiation is anticipated to be limited to any additional clauses that an organisation elects to include in its templates. However, escalation points may become more relevant if the organisation or its counterparties attempt to re-negotiate non data protection clauses/commercial terms as part of the exercise.

An organisation's playbook can be easily created, edited and maintained using specialised contract management software. Having this stored digitally can be very helpful, as the organisation can avail of technology to identify contractual clauses that have been used incorrectly and it can also be used to create new contracts or edit current agreements. This will save the organisation a significant amount of time and money over the longer term.

With the playbook complete, you should identify and review all existing contractual templates for data processing (DPAs). Because the New SCCs cannot be modified and they will take precedence over other contract provisions, it is not sufficient to simply replace the Old SCCs with the New SCCs.

Instead, organisations must undertake a review of existing DPAs to identify and amend or remove any conflicting provisions. As above, this can be achieved much more quickly when the organisation deploys appropriate contract review software. For example, legal software that can organise all agreements by contract type, meaning that the project team will not have to spend time trying to identify all of the DPAs as they will always be in one place. Organisations should consider software with the functionality to automatically identify contracts within which the Old SCCs are contained.

This is useful as a validation exercise to ensure all relevant contracts have been updated and no longer include the Old SCCs.

Repapering

New Contracts (continued)

Once the review of template documentation is complete, all existing standard templates should be updated with the appropriate version of the New SCCs (i.e., with the correct module included) for the relevant category of relationship as per the playbook.

To ensure consistent and correct application of the clauses, all employees / contractors involved in the contractual process should be trained on the New SCCs and on the organisation specific playbook.

Note:

Where employees in business units outside of the legal team issue and negotiate contracts, they should also be involved in this training – for example, sales team members. All relevant individuals should clearly understand how the New SCCs apply, on what terms there is room to negotiate and the circumstances in which they should seek approval for deviations from the approach set out in the playbook.

Existing contracts

Once the necessary documentation and processes are in place to ensure compliance with the 3-month window for application of the New SCCs to new data transfers, organisations should quickly turn their attention to putting a plan in place for updating existing arrangements within the 18-month window allowed.

If not completed as part of the data mapping exercise discussed previously, organisations should rapidly look to first identify all relevant data transfers, along with the associated contracts and counterparties. You should be working off a definitive list of all relevant transfer arrangements, the counterparty, what contract applies to the arrangement, where that contract is located and within which relationship category the arrangement fits (i.e., controller to controller, controller to processor, processor to controller or processor to processor).

All relevant contracts will need to be reviewed to identify key provisions, as outlined below. Depending on the industry, the nature of the data being transferred and any specific other considerations relevant to a particular business, organisations may wish to also incorporate additional provisions in their review.

Repapering

Existing contracts (continued)

Elements of review:

- Termination / expiry / renewal dates.
  - What is the term of the contract, when does it expire, does it auto-renew, do the parties have termination for convenience rights?
- Amendment provisions.
  - What is the contractual mechanism for amendment of the contract? Is consent required, can one party unilaterally amend the DPA etc?
- DPAs.
  - As above, organisations must undertake a review of existing DPAs to identify and amend or remove any provisions that conflict with the New SCCs.
- Counterparties.
  - Specific legal entities along with contact details if specified.
- Governing law and jurisdiction.

Again, at this point, it is worth considering the use of contract review software when undertaking this exercise as it means that the time required to complete the review can be greatly reduced. The clauses above can be found quickly and easily, removing legal risk, and provisions can be amended at the click of a button. Additionally, important dates around terminations and renewals can be diarised to generate automatic email reminders.
With the review completed, organisations should look to define a project plan for updating the existing arrangements. This project plan should include:

- Details of all contracts requiring amendment within the 18-month window. Note for transfer arrangements expiring within the 18-month window that it is not anticipated will continue or renew, no action is required to be taken. Where feasible, organisations may also elect to move certain data transfers to keep them within the EEA and avoid the need to use the New SCCs for those transfers (and associated compliance requirements).
- Prepare an evaluation template and use it to evaluate each transfer arrangement where the New SCCs will need to be applied, grading each evaluation in terms of level of risk, business impact and complexity.
- Categories of contracts to be amended along with applicable New SCCs. Each contract to be amended should be classified based on the relevant importer/exporter relationship. If not developed earlier, an organisation should have a playbook clearly setting out which module of the New SCCs applies to each such category (including any additional clauses required).
- Other amendments. To the extent the organisation has identified any potential opportunistic commercial or other provisions for negotiation, the project plan should detail the proposed other amendments and the contracts to which those apply.

Repapering

Existing contracts (continued)

- Timing for amendment. Organisations should consider a few factors when determining the order and timing for any amendments:
  - Renewal dates. If a contract is up for renewal within the 18-month window, it may be sufficient to wait and approach amendment of the Old SCCs along with the general contract renewal negotiation.
  - Nature of the counterparty. If it is anticipated that any amendment process may be lengthy, for example because of the size of the counterparty, it would be prudent to prioritise those negotiations.
  - Approach to amendment. If the organisation is taking the opportunity to renegotiate or amend other provisions of the contractual framework (such as commercial terms), parties should build in additional time for those negotiations.
  - Priority. The organisation may wish to prioritise transfers by order of significance based on the earlier evaluation, whether because of the volume, complexity or sensitivity of the data being transferred or because the jurisdiction to which the data is being transferred is likely to require a more involved transfer impact assessment.
- Stakeholder engagement. The plan should detail how it is intended to reach out to relevant counterparties, along with how those relationships are owned within the organisation currently and any relevant considerations in the engagement.
- Resources. The plan should identify all resources required to implement the project within the required timeframe, including technology and personnel, as well as any other key dependencies.

What to do next?

Timing is critical

The first deadline is 27 September 2021, to be prepared to meet that deadline, there is a substantial body of work to be undertaken. To minimise the operational burden, organisations should immediately begin planning for implementation of the New SCCs with a long lead time, to maximise synergies with their existing privacy programs and take advantage of natural contract renewal cycles.

At this stage, organisations should also be thinking hard about the resources required to execute on the project. A mix of advisory and project management skills will be required, do you have those resources available internally or will you need external support?

Dependent on the complexity of an organisation's data flows, even with the necessary skills inhouse, there may not be sufficient internal capacity to execute on the project plan. In that case, organisations should consider how to bring in appropriate external support to manage and execute on the project.

When considering the mix of resourcing required, a project like implementation of the New SCCs is ideal for applying a right sourcing approach, involving a mix of advisory, process and technology for the most cost effective and appropriate execution.

Organisations are battling numerous complex regulatory updates and may feel they have limited bandwidth to tackle implementation of the New SCCs. However, ignoring or delaying the project is likely to be costly.

Without the right combination of support, organisations may end up having to engage law firms to execute on the full project, paying advisory rates for largely administrative and project management work.

Failure to comply on the other hand can result in significant penalties, including of up to €20 million ($24.23 million) or 4% of annual turnover if you continue to transfer data without a valid legal instrument (Article 83(5)(c) GDPR).

The Johnson Hana Solution.

Johnson Hana has partnered with leading technology providers, Summize and One Trust, to offer an end-to-end solution to organisations to achieve compliance with the New SCCs. We provide clients with a truly holistic methodology which uses experienced legal professionals, proven project management practices and leading technology to provide an efficient, reliable service.

Depending on client requirements, we can provide bespoke managed solutions for all or a selection of the elements of the requirements of the New SCCs. We will tailor the level of support required as is appropriate for our clients. For example, we can provide assistance on the full repapering exercise or only for certain contracts or transfer arrangements which are particularly complex, sensitive or large in scale.

Our model is designed to provide ultimate transparency on progress, cost and timelines throughout any engagement with our clients. With any Johnson Hana solution, our clients will benefit from dedicated project managers who will design a reporting framework tailored for each client, ensuring our clients have full clarity on progress and certainty over costs incurred to date and expected future costs.

Data Mapping

We can work with you to conduct a comprehensive data mapping exercise, providing the framework within which to do so, template documentation and project management to ensure that the exercise is completed thoroughly and within the required timeframe. Our partner One Trust provides technology that can be used to automate data mapping exercises, if required, depending on the complexity and volume of an organisation's data flows, and our project managers are fully accredited on their systems to assist with implementation of relevant software modules.

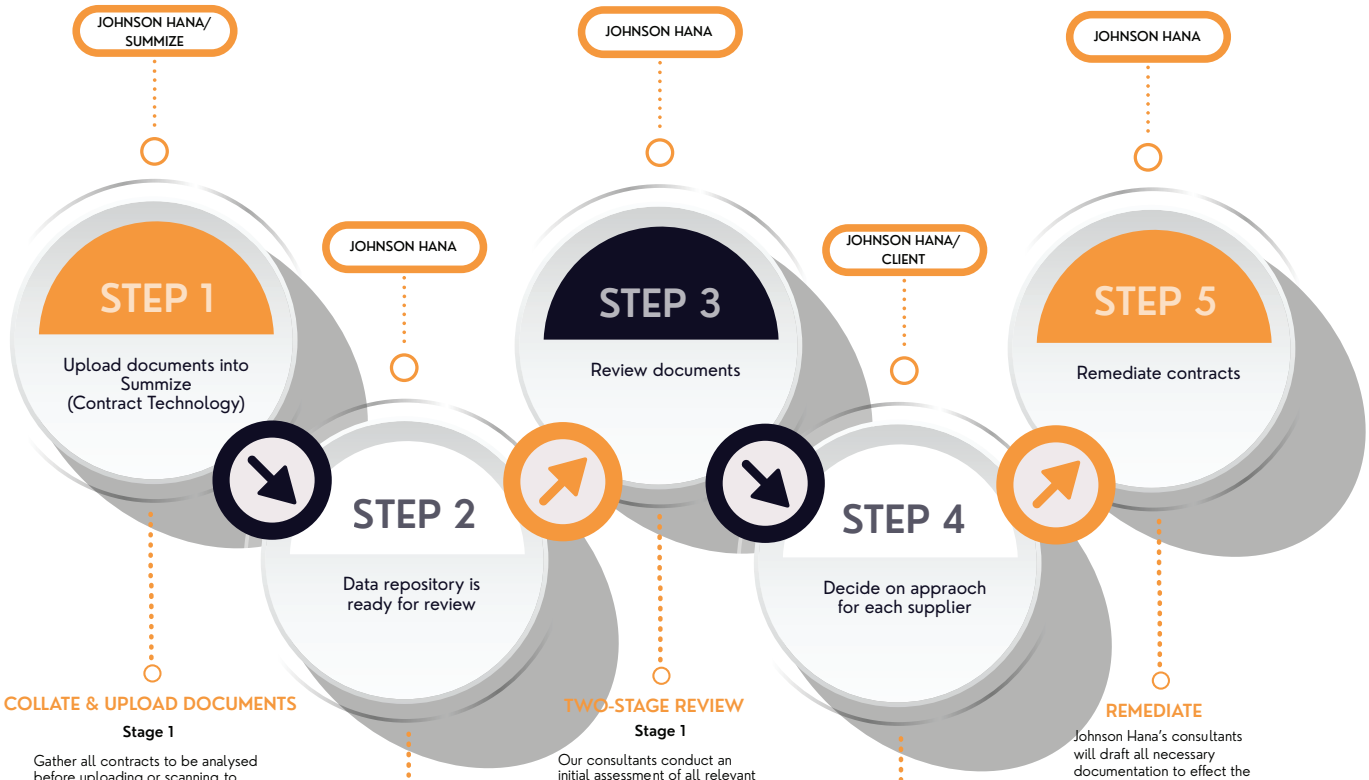
Transfer Impact Assessments

We will be working with One Trust, the leading international privacy, security and governance organisation, to provide solutions for clients on the TIAs. As well as working with organisations to establish the procedures and methodology required to operationalise TIAs, we can provide templates for conducting assessments as well as third country risk profiling.

The Johnson Hana Solution.

Repapering

Johnson Hana will work with you to create the playbook referred to above, as well as put in place the project plan required to actually implement the repapering project. We assist in the update and implementation of data protection compliance programs. With our extensive experience in this area, we provide templates which can be quickly adapted to your needs. We will work directly with you to put these plans and processes in place and are also happy to work collaboratively with your other external advisors as required.



COLLATE & UPLOAD DOCUMENTS

Stage 1

Gather all contracts to be analysed before uploading or scanning to Summize.

Stage 2

In Summize, data is extracted and verfied using:

- Optical Character Recognition
- Artificial Intelligence
- Machine Learning

This then goes to the Data Processesing team for verification and labelling.

DATA REPOSITORY

The Johnson Hana team would have access to all applicable contracts in one centralized location, their key clauses identified and the ability to comment, share and amend any terms within.

TWO-STAGE REVIEW

Stage 1

Our consultants conduct an initial assessment of all relevant contracts and data protection agreements to identify whether data is transferred outside EU.

Stage 2

Where data is transferred outside of the EU, analysis is carried out to determine the existing safe transfer mechanism being relied upon.

DECIDE

Johnson Hana will work with you to agree on the best approach for each relevant transfer, including:

- evaluation of transfers, determination on transfers requiring amendment;
- categorisation of contracts for amendment and prioritisation of negotiations;
- any other amendments to be sought; and
- counterparty and stakeholder engagement plan.

REMEDIATE

Johnson Hana's consultants will draft all necessary documentation to effect the agreed amendments and will engage with the transfer counterparties to negotiate the amendments.

Summize

Johnson Hana.

The Johnson Hana Solution.

Repapering (continued)

We will deploy our legally qualified professionals to conduct the contract review and prepare amendments as required. Johnson Hana has partnered with Summize, an easy-to-use contract solution, to review a high volume of contracts, facilitating the rapid creation of a schedule of the key contractual clauses. This seamless process significantly reduces the level of hours required for manual review and, in turn, significantly reduce costs.

Ongoing / Business As Usual (BAU)

Outside of the initial compliance burden, organisations should also be thinking about managing the ongoing issuance and negotiation of data processing agreements following implementation of the New SCCs. Johnson Hana provides managed solutions to clients to support them in relation to their business-as-usual contracting – we anticipate that, rather than investing significant resources in training legal and sales professionals, many clients will look to outsource the ongoing preparation and negotiation of data processing agreements to manage capacity internally and ensure that internal teams are free to focus on their core competencies.

A Tailored Process

To discuss how we could tailor this process to suit your requirements, please get in touch: info@johnsonhana.com

Johnson Hana.

Contact us.

We can help you.

Thank you for reading our whitepaper, we hope you've found it helpful.

Now that you've taken the time to consider what your requirements are, we would welcome the opportunity to discuss how we can help.

Contact Info

+353 1 514 3613

www.johnsonhana.com/contact/

info@johnsonhana.com

2 Dublin Landings, North Wall Quay,
North Dock, Dublin 1

Disclaimer

Johnson Hana.