Johnson Hana.

Replacement Standard Contractual Clauses (the New SCCs)

How to conduct the repapering exercise

June 2022

An examination of the repapering exercise companies must complete to comply with the New Standard Contractual Clauses.

Table of Contents

Introduction

Six months to go.

With the final deadline on the 27th December, time is running out.

To comply with the “Schrems ii” ruling, all companies must replace all their existing Standard Contractual Clauses (SCCs) with the “New SCCs” published by the European Commission on 7 June 2021.

This means an extensive repapering exercise for many companies. This must be completed by 27 December 2022. Companies who do not meet this deadline risk non-compliance with GDPR.

With six months to go, this whitepaper serves as a guide to show how this can be completed.

Step one

Data Mapping.

What a Data Map looks like, and how to build one

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.

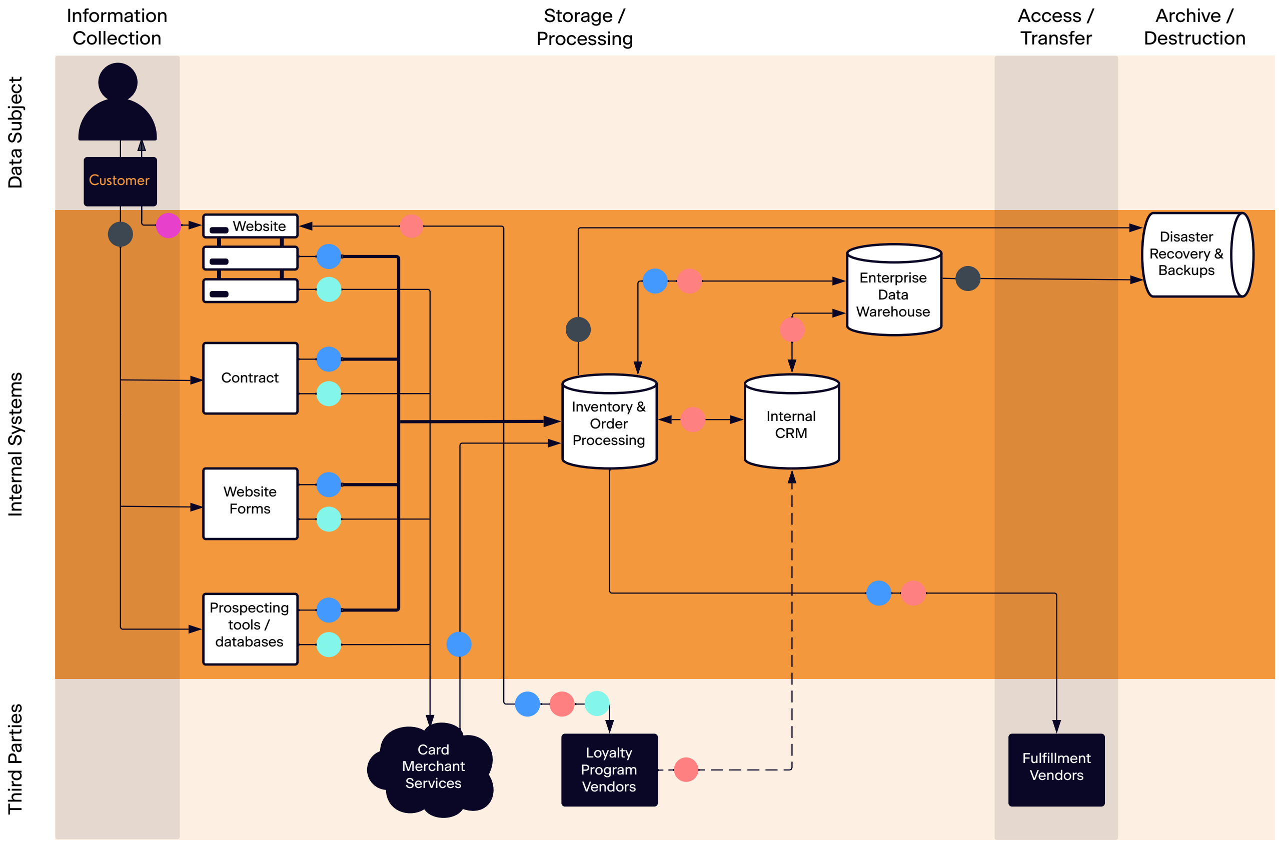
Sample Data Flow Map

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

Depending on the complexity of how and where data flows through a company, the size and scale of these data flow maps can vary widely.

Compiling this map is therefore an important initial exercise as it will give a broad indication of the magnitude of the task at hand.

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.

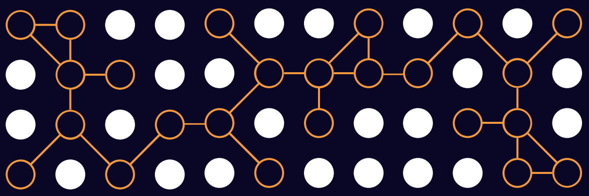
- For each counterparty, you should determine in what capacity each of you is acting with respect to the personal data in question, i.e., as a data controller or data processor? Having this element of the data mapping done will be crucial to understanding which module of the New SCCs is required for 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.



Step two

The Repapering Exercise.

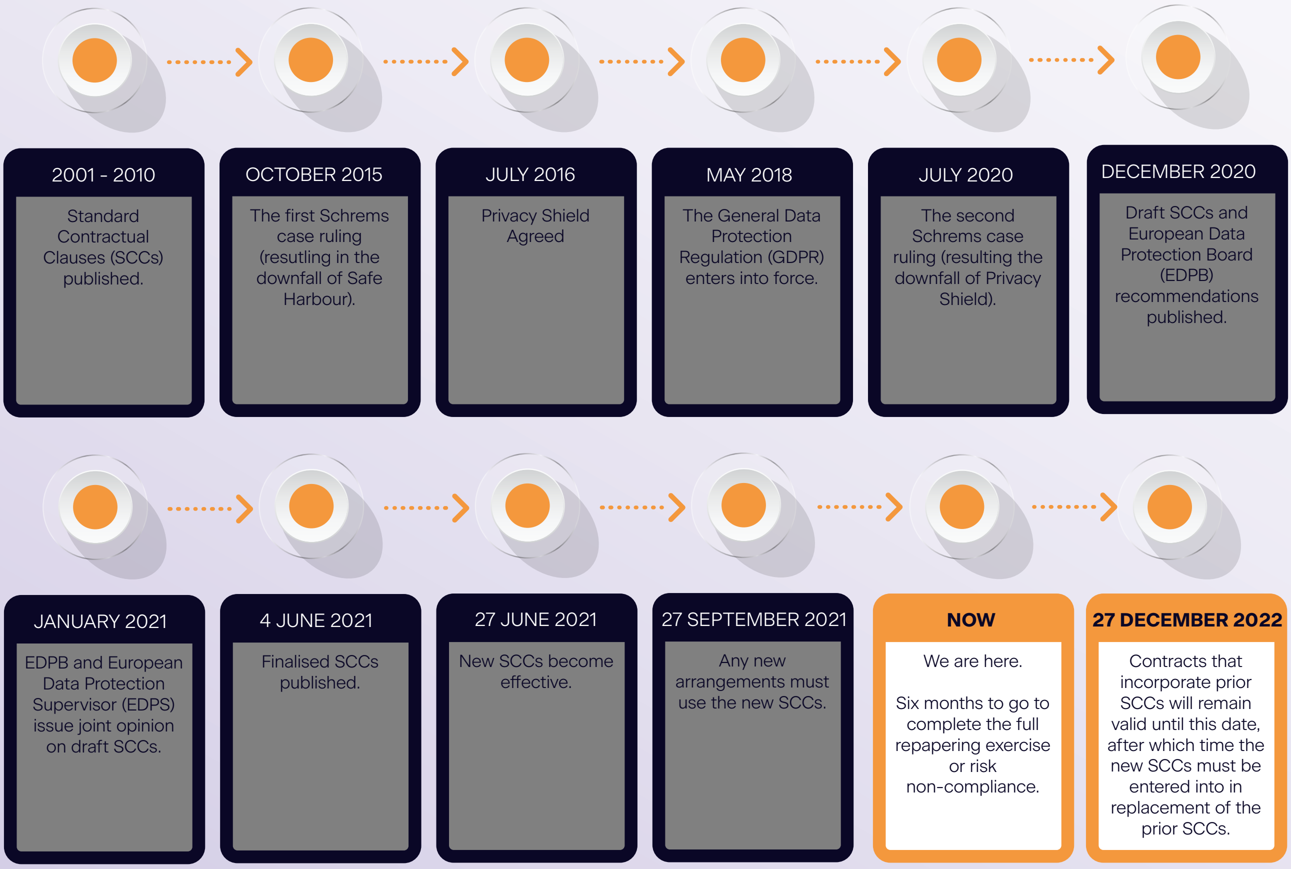
Repapering

Timelines

The critical deadline for the practical implementation of the New SCCs is 27 December 2022.

The New SCCs were published in the Official Journal on 7 June and took effect on 27 June 2021. The Old SCCs remained valid and effective until they were repealed on 27 September 2021 - until then, organisations were entitled to continue to use the Old SCCs for all new transfer arrangements entered into.

For existing arrangements under the Old SCCs, organisations have a six month window remaining, until 27 December 2022, to replace the Old SCCs with the New SCCs for those transfers.



2001 - 2010

Standard Contractual Clauses (SCCs) published.

OCTOBER 2015

The first Schrems case ruling (resutling in the downfall of Safe Harbour).

JULY 2016

Privacy Shield Agreed

MAY 2018

The General Data Protection Regulation (GDPR) enters into force.

JULY 2020

The second Schrems case ruling (resulting the downfall of Privacy Shield).

DECEMBER 2020

Draft SCCs and European Data Protection Board (EDPB) recommendations published.

JANUARY 2021

EDPB and European Data Protection Supervisor (EDPS) issue joint opinion on draft SCCs.

4 JUNE 2021

Finalised SCCs published.

27 JUNE 2021

New SCCs become effective.

27 SEPTEMBER 2021

Any new arrangements must use the new SCCs.

NOW

We are here.

Six months to go to complete the full repapering exercise or risk non-compliance.

27 DECEMBER 2022

Contracts that incorporate prior SCCs will remain valid until this date, after which time the new SCCs must be entered into in replacement of the prior SCCs.

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 six months remaining to the 27 December deadline, organisations should prioritise new SCC compliance as a matter of utmost urgency.

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

Playbook Creation

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, 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

Playbook Creation (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.

Repapering

Playbook Creation (continued)

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.

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.

Repapering

Implementation phase

Once the necessary documentation and processes are in place (if they are not already), organisations should urgently turn their attention to putting a plan in place for updating existing arrangements before the deadline.

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.

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.

Repapering

Implementation phase

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 six month window. Note for transfer arrangements expiring within the six 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

Implementation phase (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 six 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.

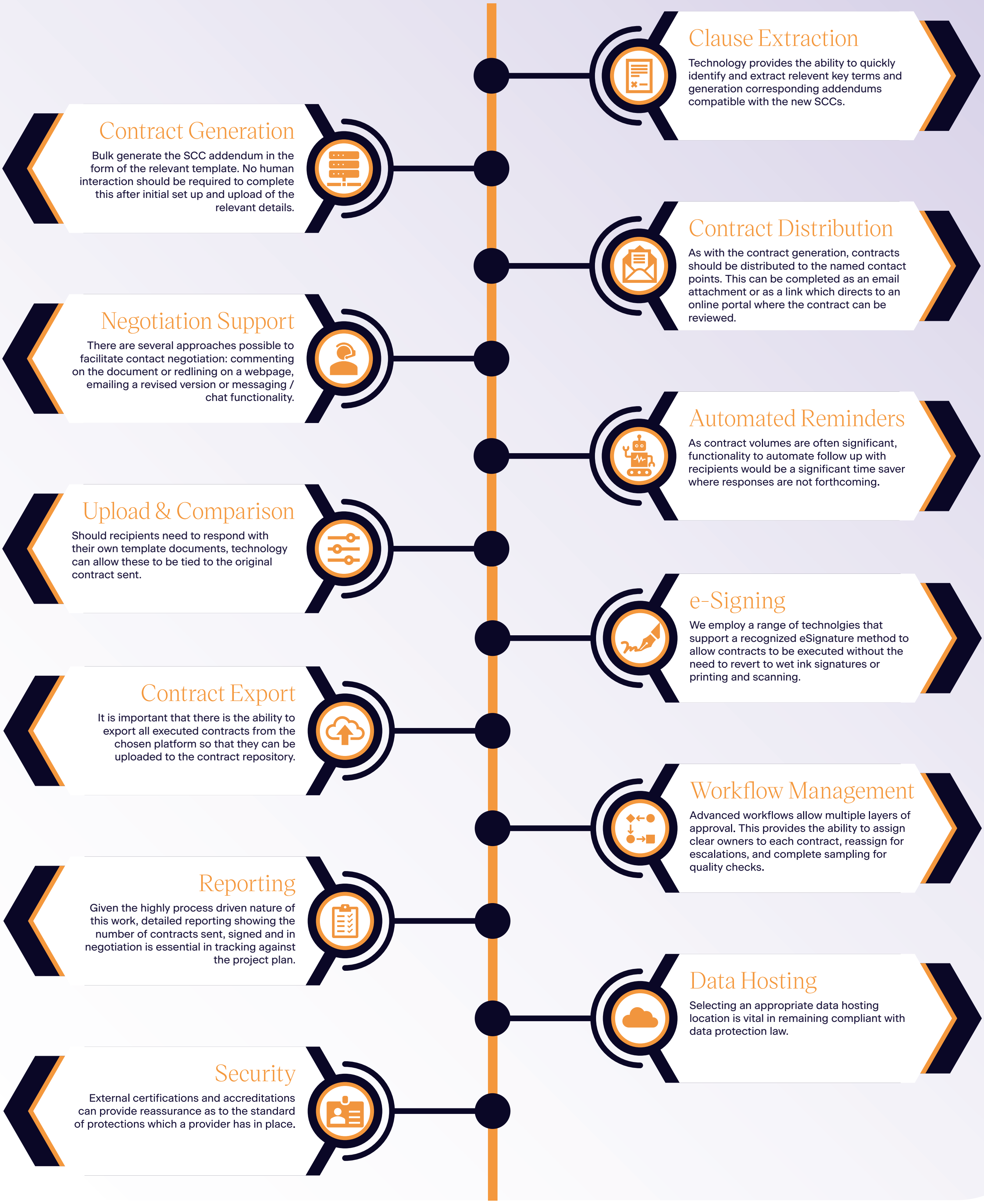
    - Priority. The organisation may wish to prioritise transfers by order of significance based on the earlier evaluation, whether because of the volume, complexity or sensitivity of the data being transferred or because the jurisdiction to which the data is being transferred is likely to require a more 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.

Technology workflow.

At Johnson Hana, we use the right technology to support our people in delivering an efficient, high-quality outcome. We do not utilize technology for its own sake and will recommend low or no tech approaches when it is appropriate. Below is a sample of workflow demonstrating some of the possible benefits of using technology on an SCC repapering project.



Clause Extraction

Technology provides the ability to quickly identify and extract relevent key terms and generation corresponding addendums compatible with the new SCCs.

Contract Generation

Bulk generate the SCC addendum in the form of the relevant template. No human interaction should be required to complete this after initial set up and upload of the relevant details.

Contract Distribution

As with the contract generation, contracts should be distributed to the named contact points. This can be completed as an email attachment or as a link which directs to an online portal where the contract can be reviewed.

Negotiation Support

There are several approaches possible to facilitate contact negotiation: commenting on the document or redlining on a webpage, emailing a revised version or messaging / chat functionality.

Automated Reminders

As contract volumes are often significant, functionality to automate follow up with recipients would be a significant time saver where responses are not forthcoming.

Upload & Comparison

Should recipients need to respond with their own template documents, technology can allow these to be tied to the original contract sent.

e-Signing

We employ a range of technolgies that support a recognized eSignature method to allow contracts to be executed without the need to revert to wet ink signatures or printing and scanning.

Contract Export

It is important that there is the ability to export all executed contracts from the chosen platform so that they can be uploaded to the contract repository.

Workflow Management

Advanced workflows allow multiple layers of approval. This provides the ability to assign clear owners to each contract, reassign for escalations, and complete sampling for quality checks.

Reporting

Given the highly process driven nature of this work, detailed reporting showing the number of contracts sent, signed and in negotiation is essential in tracking against the project plan.

Data Hosting

Selecting an appropriate data hosting location is vital in remaining compliant with data protection law.

Security

External certifications and accreditations can provide reassurance as to the standard of protections which a provider has in place.

Practical tips.

Having supported and undertaken multiple repapering projects for clients, we wanted to share some practical tips and lessons learned. Oftentimes, the best laid project plans can fall down on seemingly small but unforeseen issues, and given the limited time remaining to comply with the repapering obligations, an effective project should consider and plan for these issues up front.

Playbook, Module Selection & Amendments

1. **Holistic Understanding of Contractual Framework**

   Contract v SCCs
   Generally the SCCs will only form part of a broader contractual relationship. The EC requires that organisations review those contracts to ensure that nothing in them contradicts the text of the SCCs. Rather than conducting this potentially time-consuming review and amendment, organisations may wish to simply state that the new SCCs will take priority over and supersede any conflicting provisions.

   Termination
   The SCCs entitle the data exporter to terminate the transfer of personal data in certain circumstances. Parties should consider the interplay between this and the termination rights in the broader commercial contract. If the transfer of personal data can be halted, can the commercial contract be fulfilled? Who is exposed in that situation? Customers who are data exporters may find themselves in a situation where they must halt the transfer of data to their data importer vendor under the SCCs, but without a corresponding termination right under their services agreement, leaving them potentially exposed for charges for a service that they are unable to use.

2. **Multiple Relationships**
   Some parties may act in multiple different relationships with each other for different transfers and the EC has confirmed that multiple modules can be used in those circumstances. Parties may take a liberal interpretation by incorporating all modules and stating that the relevant one will apply depending on their respective roles rather than reviewing each transfer and specifying which module applies.

Counterparty Engagement and Negotiation

1. **Contact Details**
   A small but often ill thought through detail is the requirement to have clean, up to date contact details for counterparties. Amendments will need to be directed to the right person, with a valid email address, in the counterparty to ensure that the agreement can be reviewed and signed off on in a timely manner. Incorrect details can result in large numbers of bounce backs, or amendments landing in unsuitable inboxes where they languish uncompleted. On projects involving large numbers of contracts to be repapered, these issues can cause significant delays. Organisations should be asking themselves whether they have contact details for each of their counterparties to send the amendment to, and whether they are confident in the accuracy and suitability of those details. Where confidence is low, project plans should build in some level of testing to assess the data and perform a data cleanse where necessary in advance of commencing the dispatch of amendments.

2. **War of the Papers**
   Many organisations will find that having invested significant time in developing their own preferred template to execute, on engaging with a counterparty that organisation is insisting on using their own template, potentially with differences in modules and annex details. A good project plan should anticipate this scenario and have an agreed framework for dealing with such requests. Where would such a request be considered? If counterparty paper is to be accepted, does it need to be reviewed and by who? How do the proposed project resources (people, technology and processes) fit that situation?

Practical tips (continued).

3. **Redlines / Approach to Negotiation**
   We are seeing significant scope for negotiation, notwithstanding that the text of the SCCs themselves may not be changed. Application of modules is questioned, and different counterparties to the relationship may find that they have different ideas of how the annexes should be completed.

   Organisations should be well set up to deal with negotiations from commencement – asking themselves the following questions:

   - Are you allowing redlines?
   - What aspects do you expect to be negotiated?
   - Are your negotiators trained on those points? Do you have approved fallback positions / alternatives?
   - What are the escalation points for approvals?

4. **Execution**
   Organisations should consider how they will actually execute the SCCs – will electronic signature be used? Will they consider pre-signed contracts? Note EC guidance on the topic:

   > *The use of the SCCs to fulfil the requirements of the GDPR and EUDPR for the controller-processor relationship, or as a transfer tool, requires that the parties enter into a legally binding agreement to abide by them. To this end, the parties need to fill in the annexes to the SCCs and sign Annex I, which form an integral part of the clauses. Inter alia, the parties have to provide their contact details and information on their respective roles (who acts as controller and processor, or data exporter and data importer) under the clauses. The SCCs do not contain any requirements on how the signature should be formalised (e.g., whether it can be done electronically). This is left to national (civil/contract) law governing the agreement.*

   We have had clients considering unilateral imposition of revised SCCs, some implementing clickwrap, all the way through to full negotiation and execution (whether physical or electronic). In each case, it is for the organisation to satisfy themselves that they meet the requirements for a legally binding agreement to be created and signed by both parties.

Technology

Technology tools can be very helpful in automating aspects of the process and reducing the volume of manual work to be undertaken. However, organisations should be careful to first design their project plan and preferred process map and use that to dictate where technology can best be deployed to actually drive material efficiencies.

Depending on the details of the particular project (volume, level of expected negotiation, nature of the counterparties, governing law / jurisdiction etc), some of the technology capabilities that we have seen the best use cases for are bulk contract creation and sending, having a single platform for negotiating and signing and electronic execution.

Organisations should also consider whether there is sufficient benefit to consider licensing specialist technology for the platform, or whether any functionality in existing internal systems could be deployed on the project.

Finally, remember to be careful to check where your data is being hosted if relying on any cloud hosted technology – many of the CLM solutions are hosted in the US and organisations may find themselves inadvertently transferring further personal data outside the EU.

What to do next?

Timing is critical

The deadline is 27 December. From the date of publication of this whitepaper, that leaves exactly six-months.

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 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

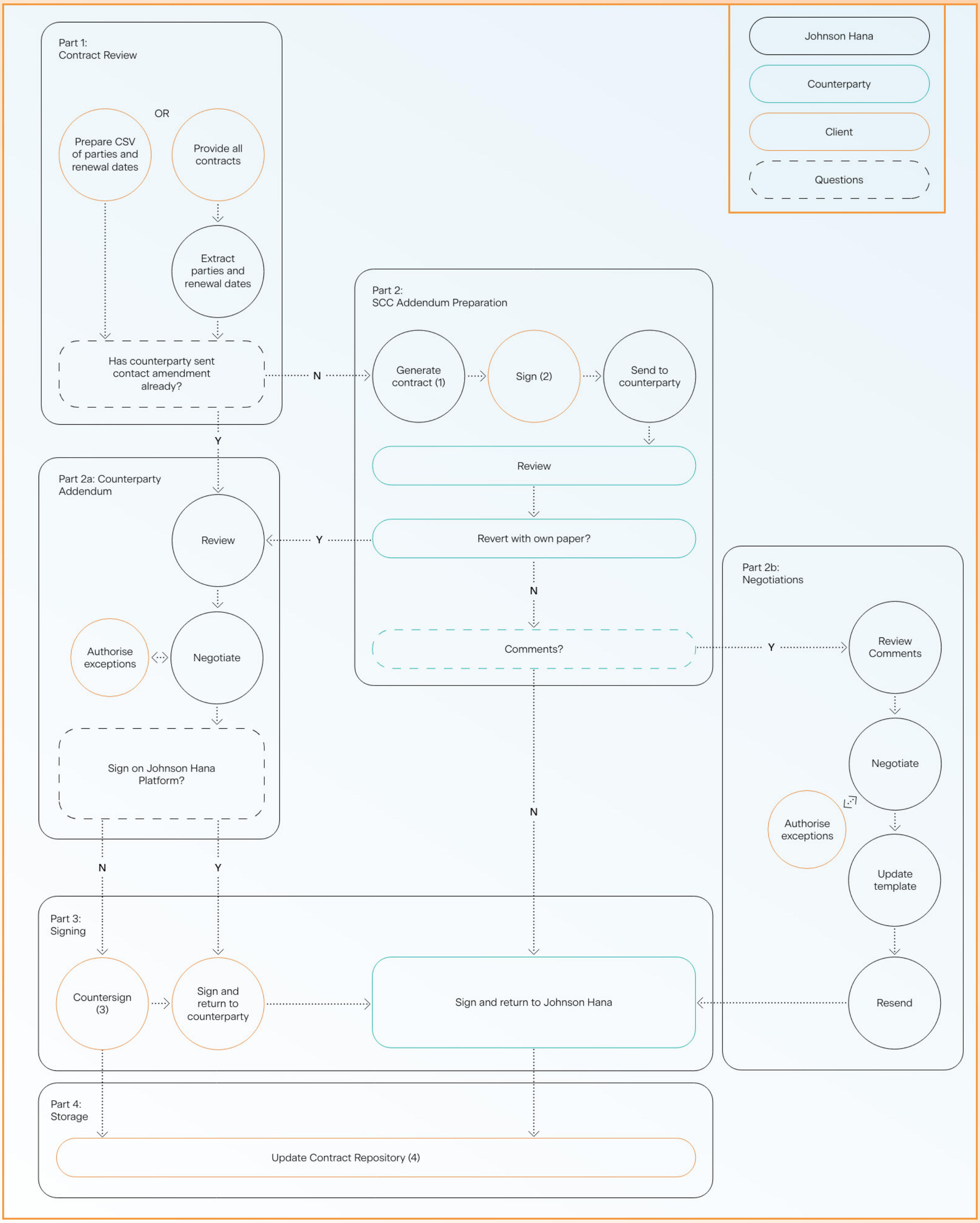
We can work with you to conduct a comprehensive data mapping exercise, providing the framework within which to do so, template documentation and project management to ensure that the exercise is completed thoroughly and within the required timeframe. Our partner One Trust provides technology that can 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.

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.

The Johnson Hana Solution.

Repapering Process Flow



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
📍 21-23 Fenian St, Dublin 2

Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. It does not purport to constitute legal advice and should not be relied upon by any party. Please note that Johnson Hana does not provide legal advisory services.

Johnson Hana.