www.pwc.ch

Data protection within new technologies: blockchain

Is your personal data secure when processed on a blockchain?

pwc

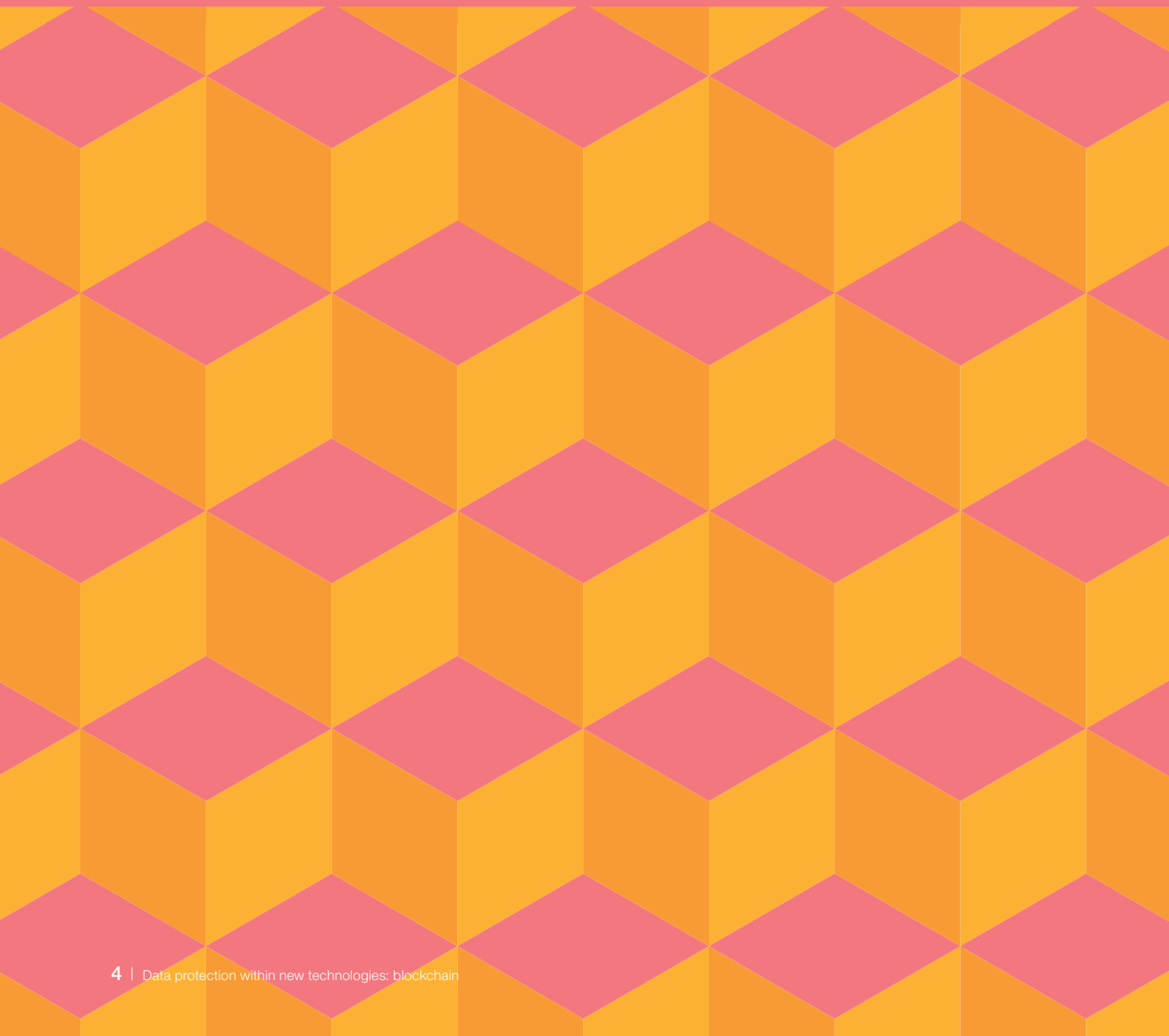
> “The blockchain cannot be described just as a revolution. It is a tsunami-like phenomenon, slowly advancing and gradually enveloping everything along its way by the force of its progression”

William Mougayar

New personal data processing technologies - introduction

Companies have been processing personal data for decades, using technologies that have seen an exponential sophistication. Data that was once collected and stored in a simple databas, is today segmented, analysed, processed and augmented by a number of different systems. People constantly give access to their personal data, and have often no idea where their data will be processed, how, or even for how long. And this becomes increasingly true with the new technologies coming into the market today: artificial intelligence, machine learning, blockchain – chances are your personal data is consumed on a daily basis by systems leveraging one or all of those systems, and the likelihood is that you know very little about what happens to your data after all.

A number of regulations are in place aiming to ensure that, regardless of your understanding of the technology processing it, your personal data is kept safe and used only for legitimate purposes – the question is: are these regulations up to the challenge?



Personal data protection regulations

More ways to process personal data naturally translate into more possibilities to misuse such data for whoever has access to it (legally or illegally). Cases of misuse of personal data, or data breaches, are frequently in the news, and this explains why this topic is very high in the agenda of a number of governments world-wide. In many countries, regulations to protect personal data have been recently introduced or updated, as shown in the table below, where we present a selection of countries and their recent developments in this area.

What is interesting to notice, is that in many cases the regulations have been revisited to be in line with the recently published EU General Data Protection Regulation (GDPR) – which is broadly seen as the golden standard when it comes to regulations on the protection of personal data.

Country	Key privacy regulation	New or updated law	Similarity to the GDPR	Timeline
Switzerland	Federal Act on Data Protection	Updated	High degree of similarity	Expected to be fully applicable by end of 2020
Canada	Digital Privacy Act	Updated	Updates in line with GDPR requirements	Latest updates applicable from end of 2018
China	Chinese National Standards on Information Security Technology – Personal Information Security Specification	New	Some requirements are even more rigorous than the GDPR	Came into force from May 2018
India	Draft of the Personal Data Protection Bill	New (draft)	In its current state, lower protection of personal data compared to the GDPR	Draft was submitted in July 2018
Thailand	Draft of the personal data protection act	New	Designed to be aligned with GDPR	Text was approved at the end of February 2019
Singapore	Personal Data Protection Act	Existing (under review)	Similar level of protection as the GDPR	Text is currently being reviewed for increased alignment with GDPR
US[1]	Varies per state	New and updated	Varies per state	n/a

[1] It is worth mentioning the The California Consumer Privacy Act (CCPA), which is a bill that enhances privacy rights in California, and is in some aspects aligned with GDPR.

GDPR in a nutshell

Demand for the new European Union General Data Protection Regulation (EU GDPR) arose out of a need for stronger regulatory requirements regarding personal data protection. GDPR needed to embrace a much wider scope of requirements compared to the previous Data Protection Directive 95/46/EU adopted in 1995. The GDPR was published on 24 May 2016 with a transposition period of two years until May 2018 (when it came into force). It was a new regulatory framework designed to strengthen the data privacy and protection of all EU citizens, across the EU member states and abroad.

GDPR is seen by many as a milestone in the context of data protection, as it sets a level of protection for the data subject that was unheard of before. Not only does it define strict principles of compliance when it comes to the processing of personal data, but also grants data subjects a set of rights that give them more control over how their personal data is processed. A noteworthy right is the right to be forgotten: in a digitalised society where any information seems destined to be stored forever on some server, this right grants data subjects the possibility of having their data deleted once it is no longer needed for the purpose for which it was collected. More specifically, organisations need to have the capability of deleting data from all their systems upon request (including the systems of other companies to which data has been transferred).

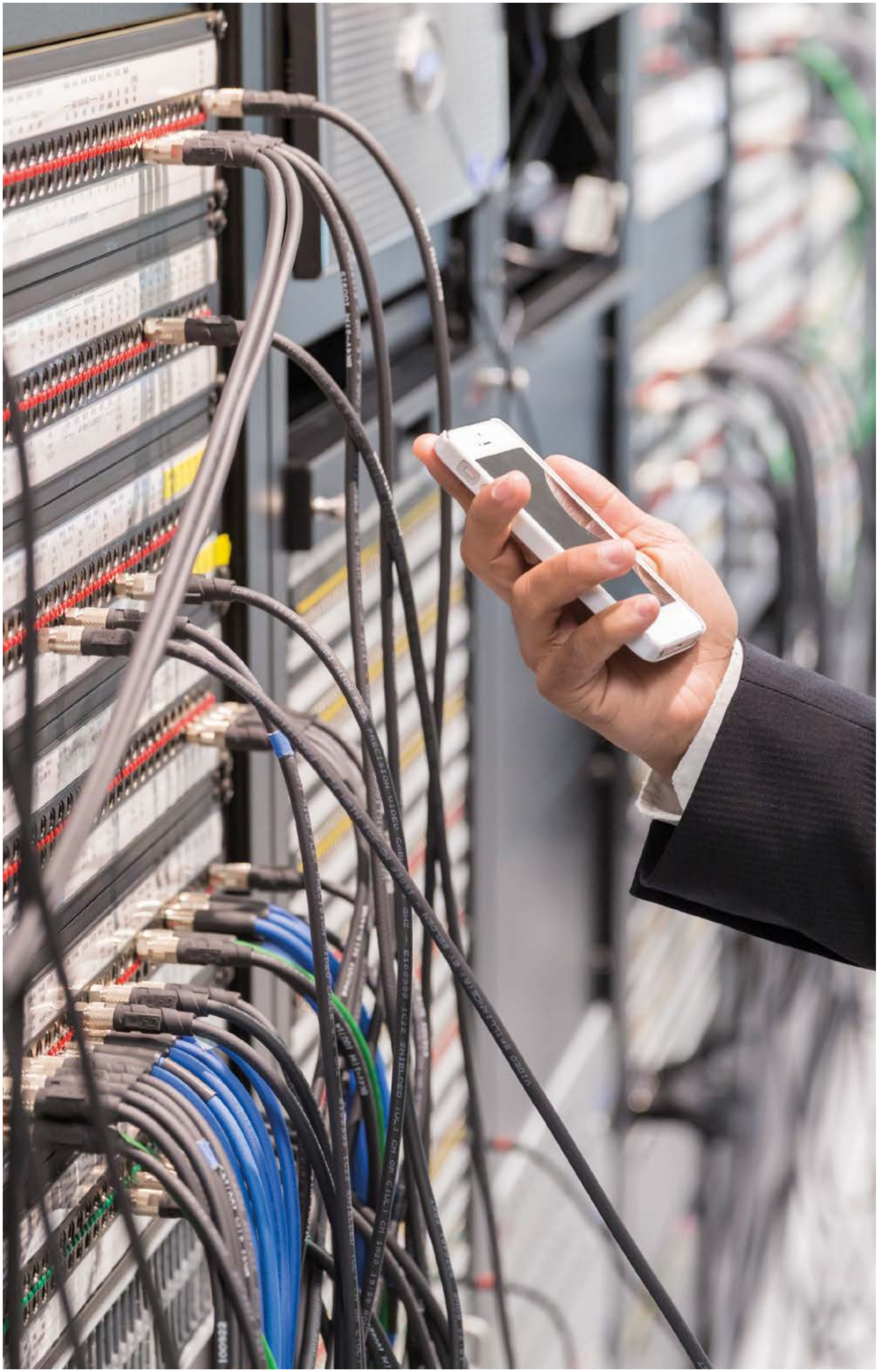
Focus point - The EU GDPR framework for compliance

The articles of the EU GDPR include a number of obligations for companies processing personal data. We have identified eight key topics that need to be covered operationally from three different perspectives: business (which data is processed), IT (where is personal data processed) and third parties (to whom is personal data transferred).

1. Data inventory Organisations need to create and maintain a data inventory to identify which personal data is processed and for which purpose.	**2. Principles** Personal data processing should always be performed in adherence with data protection pronciples (e.g. it has to be lawful, for a specific purpose, ect.)	**3. Standards** To ensure that personal data is processed in compliance with GDPR requirments, companies need to develop processes and enforce behavioural standards with their staff.	**4. Data subject rights** Under GDPR, natural persons have a series of rights (dta subject rights), to which organisations need to to be ready to answer (e.g. right of data access, or right to be forgotten).
5. Data processing records The regulation requires organisations to maintain a detailed record of all the personal data processing activities.	**6. Personal data breaches** Companies must minimise the risk of data breaches, and need to implement processes to inform the supervisory authority within 72h of a breach (when certain conditions are met).	**7. Data Protection Officer** When certain conditions are met, organisations need to nominate a Data Protection Officer to monitor compliance with GDPR requirements.	**8. Data Protection impact assessment** For processing activities which present a risk to the rights and freedom of the individuals, an impact assessment is required, to identify and implement adaquate mitigation measures.

Is GDPR future-proof?

GDPR sets a number of very specific requirements and conditions under which personal data can be processed. However, it leaves some open questions when it comes to new technologies. In this document, we will explore how effective GDPR is when it comes to protecting personal data processed by one technology that is being used more and more every day: blockchain. In itself, this is only a smart way of assembling existing technologies, however if you think that the text of GDPR has been written more than three years ago, when blockchain was not as prevalent as today, this can be a good test to check whether the regulation was written as “future-proof”, i.e. ready to be applied to any new processing technology.



Blockchain technology

Blockchain in a nutshell

A blockchain is a new type of secure database that relies on a large number of participants to derive its security. It functions as an append only mechanism, where transactional information is collected over specific time frames into a block, which will then be attached chronologically and by consensus to the general database.

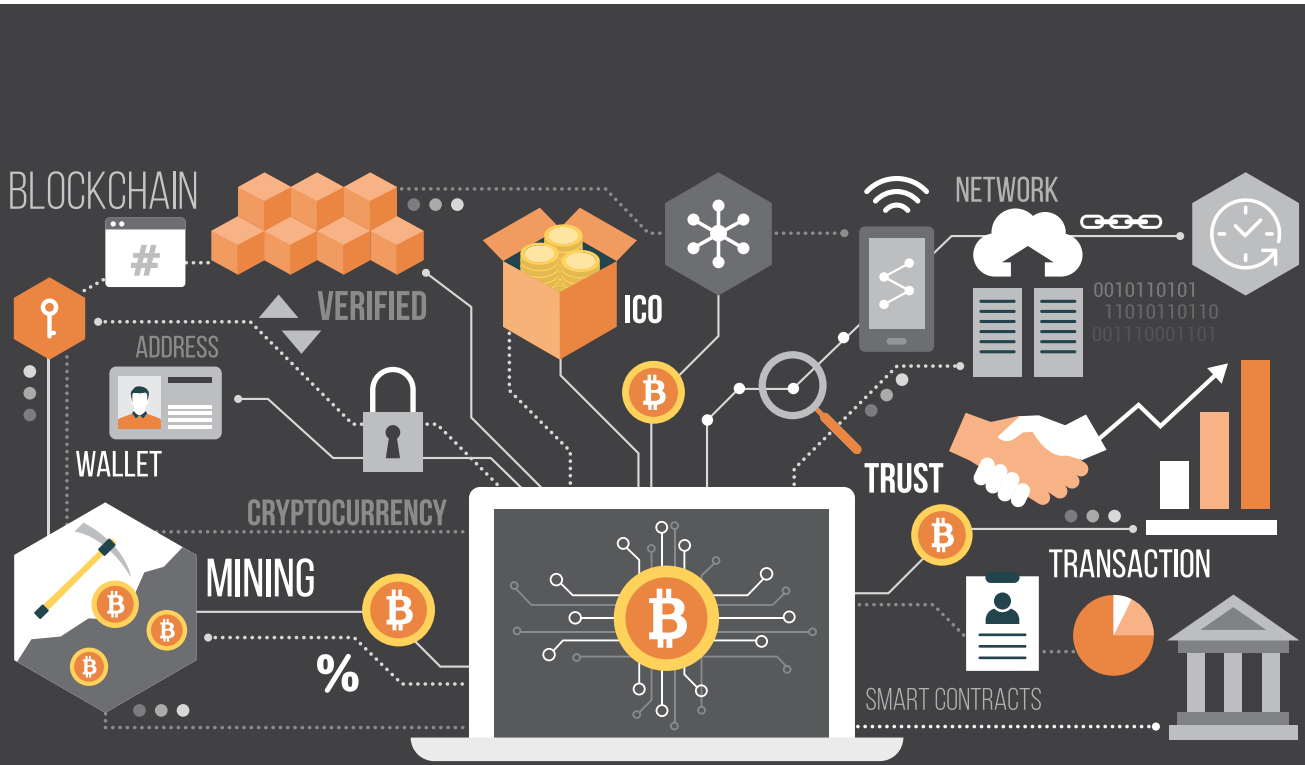
It offers to shift our double entry accounting system to a new methodology that would involve both parties in the transaction as well as the larger community of participants, recording the transaction into a block appended to the distributed database. Also, blockchain reduces the reliance on intermediaries to maintain the “single version of the truth”, as the “true” data is generally available to every participant in the blockchain and distributed in different servers to minimise the risk of data tampering.

It could form the legal framework for a borderless cyberspace jurisdiction where machines interacts with other machines through a trusted protocol. This inter-web jurisdiction will not care about the legality of the activity, but only about the validity of a transaction to be recorded on the database.

It will be up to the physical jurisdictions with which those transactions interact to decide whether the transaction is legal or not and to react accordingly.

Bitcoin, written with a capital B, is the first implementation of a blockchain and is to date by far the most secure public and participatory database in the world. One could describe bitcoins as tokens, which are created as an incentive for the participants, as a form of right to use the network or investment. This token js similar to a financial derivative, as it is essentially a digital asset which derives its value today from an external asset serving as a unit of account that can be traded.

Other examples of use cases are within the healthcare industry or a supply chain, where blockchains are leveraged to create a utility often issuing their own utility token. These type of tokens are issued solely to enable future access to the products or services offered by a company (hence, utility tokens are not created as a form of investment – although they can be traded on the basis of their intrinsic value).



Fundamentals of blockchain technology

Security
Blockchains derive their security from two major technical building blocks.

1. Distributed network - the way of sharing and synchronising data among participants - which allows participants to communicate with one another and reach an agreement around the latest state of the database by consensus. The consensus mechanisms can vary, but the major one is proof of work, which basically will depend on the amount of energy spent to solve a mathematical puzzle by a trial and error method called brute force. There is also proof of stake, where participants will put their own tokens at stake to influence the consensus which will generally be enforced by largest stake. Last but not least, there is a simple voting mechanism, called proof of authority, where a generally smaller number of participants have been identified to use their authority to vote and reach a consensus.

2. Cryptography, which helps make sure that the history cannot be modified by a participant, as each block being appended to the database will require a cryptographic reference to the previous block. Hence, if you wish to modify an earlier transaction you would be invalidating all the blocks coming after that transaction, meaning invalidating the entire chronology of the blockchain. You also use cryptography to authenticate your account and cryptographically sign a transaction and move value around.

Permissions
Blockchains have been invented to enable people without prior trust relationships to freely and securely transact with one another (without intermediaries), often with transaction fees that are a fraction of the fees for more traditional technologies. Nevertheless, many transactions in our society involve trusted regulated parties to facilitate the transaction between parties. Thus, industries have started collaborating to enable blockchains that are controlled by a “small group” of trusted participants. Permissioning of those blockchains can happen on several levels: the database can have a limited number of participants generally voting in their consensus mechanisms, it can limit the participants allowed to write or even just read the state of the database. Permissioning on any level, will “force” the qualification of the database into a permissioned blockchain.

Smart contracts
Smart contracts are contracts redacted in code, deployed and replicated to enable future self-execution. Smart contracts are used more often in connection with utility tokens (e.g. in healthcare and supply chain management), rather than security tokens. For example, Bitcoin works with redeem script, rather than smart contracts.

The key feature of smart contracts is that they will execute independently from their creator. They are nothing more than a script or program intended to digitally facilitate, verify, or enforce the obligations of a contract. They facilitate automation of business processes or contractual clauses which may be made partially or fully self-executing, enabling you to transact in a fully accountable and verifiable way while avoiding any intermediary to enforce the contract.

Blockchain technology is flexible enough to be applicable in many different situations. In the next section we will identify some typical use cases where the processing of personal data is at the core of the technology application.

Blockchain and data protection

Processing of personal data within blockchains

Given the increased security provided by the blockchain technology, one could consider using it for safer processing of personal data. Personal data would be safely stored and transferred, and an immutable record of such data would be available.

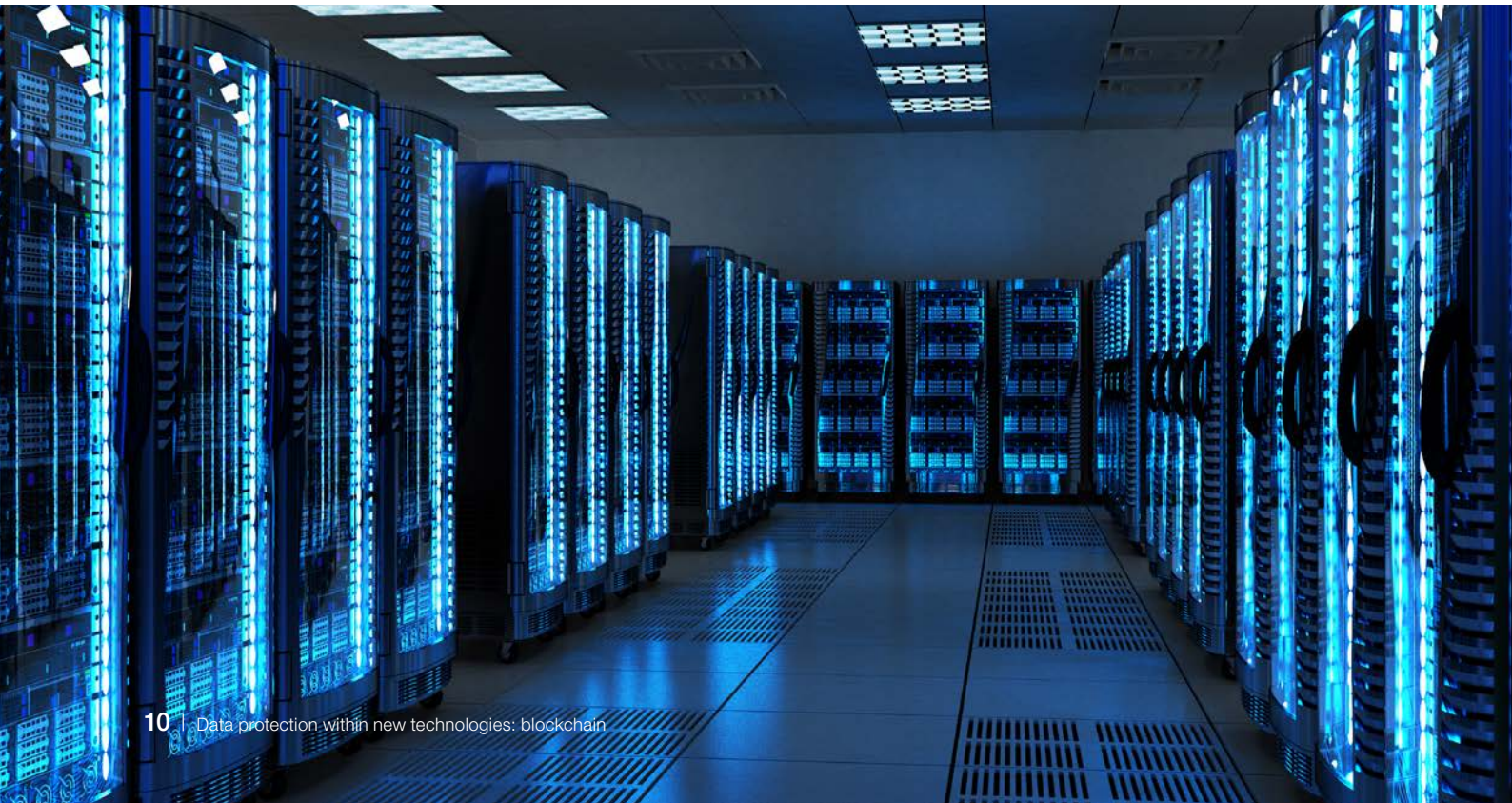
However, there are a number of reasons against this choice. In a first instance, it is important to consider the cost of blockchain: using this technology to store data is extremely expensive (compared to other types of databases), and as such this may be an economically inefficient way to store and process personal data. Second, and even more important, storing personal data on a blockchain is essentially non-compliant with many data protection regulations (e.g. GDPR), due to the nature of the technology itself (data is often transferred cross border, one cannot correct wrong or out of date data and especially data cannot be deleted).

So, although it would be technically feasible to store personal data directly on a blockchain, there are economic and compliance restrictions that one should consider before doing so. The way blockchain should be used when personal data is involved is by storing personal data in a separate database, and use a hash key (unique identifier) in the blockchain as a means to verify that certain data exists outside of the chain, and guaranteeing that data's integrity over time, rather than storing/transmitting the effective data via the chain.

Use cases

Many use cases (involving or not data protection) have emerged: from finance, gambling, process management, to certification processes, logistics, insurance, intellectual property (IP) rights and government procurement, to protecting your digital footprint through self-sovereign data and ID management, possible applications of blockchain encompass a diverse set of areas. The extent of the impact this technology will have on social interactions is still very uncertain: while some people claim it will have a radical impact on all business transactions and social interactions, others believe this is just a trend, and because of the decision power it transfers from humans to machines, people think this technology will never reach critical mass for technical as well as ethical reasons.

Here, we analyse a number of use cases where personal data processing is involved, with the purpose of identifying some of the key challenges when it comes to personal data protection and blockchain. We will try to give an answer to such challenges in the next section.



Healthcare – transmission and storage of medical records

How is the technology applied?

In the medical world many companies are working to enable patients to have better control over their own medical records and control who can and will have access to them based on exchanges of access control on a per need basis.

This is a fundamental shift, as it could enable people to be sovereign with their health records, meaning that people should be able to easily move from one practitioner to another, but most importantly they should also be able to generate revenue for sharing some of their personal records with third parties.

Blockchain also has a number of other applications when it comes to healthcare: just to give another example, the technology can make it easy to track a drug as it moves from the manufacturer to the patient. This would improve the traceability of a drug as it moves across the supply chain, and would help preventing drug counterfeiting.

How is personal data processing impacted by the technology?

The blockchain can be used as a safe transfer mechanism for sensitive data. Also, access to such data can be granted via the blockchain, which then ensures a certain level of security and integrity to the data.

What are the main challenges raised by the use case?

How to ensure sensitive data is accessed only by users with the adequate authorizations? How can a data subject maintain control of their own data, once it is shared via the blockchain?

Also, using the blockchain to store and transfer the data itself would result in the economic and compliance limitations mentioned above. Storing sensitive data in a secured database and using the blockchain only for transmitting the hash keys needed to verify such data would represent a more efficient use of the technology.

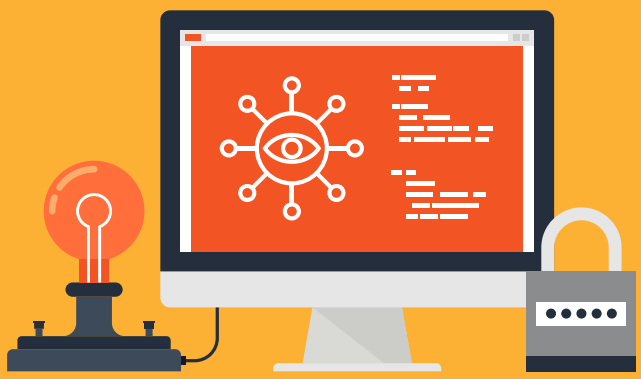
Supply chain management and fraud detection

How is the technology applied?

Blockchain is a powerful technology for increasing transparency over multi-party supply chains, and many companies depend on complex processes with numerous participants to secure the supply of raw materials all the way to finished goods. In order to improve the efficiency of such complex processes, many are looking into blockchains where sensors and sealed containers would be required to communicate with a secure and trusted database.

The use of blockchain should considerably improve trust, security, speed and should radically improve information flows across multiple parties involved in the supply chain.

Because goods attributes can be recorded and timestamped on a blockchain it would be much easier for an end consumer to verify the provenance and authenticity of the goods they buy.



How is personal data processing impacted by the technology?

Transactions can be between different businesses, but also between businesses and individuals (or even between individuals themselves). When people are involved in a transaction, personal data is often exchanged for identification purposes. Sharing personal data access via a blockchain, rather than traditional electronic means, should increase the protection of such data, and the blockchain could serve the purpose of validating the authorisations as well, reducing fraud risk.

What are the main challenges raised by the use case?

If the blockchain is used to validate the personal data exchanged, then the blockchain itself is processing personal data and as such needs to be compliant with GDPR requirements, but as a general rule personal data should not be stored on a blockchain - only a unique reference to personal data should be stored on a blockchain to guarantee integrity.

Digital services with certified personal identification

How is the technology applied?

In the digital world a lot of services cannot be used without additional personal identification. For many services one needs to send additional certified information, e.g.: a copy of a passport or ID card. This is the case for financial or government services that are subject to tight regulation. Furthermore, the ability to transfer one's personal record is currently limited, as changing a service provider, e.g. a doctor or a bank, does not allow one to transfer personal history (medical history, financial history) with the analogue ID card. If everyone had a digital version of all these records, they could take their ID everywhere and make it legally binding. A passport number, for example, could be certified by an authority to allow the user to open a bank account without scanning the passport, and only checking that the right authority has certified the right attribute required to be shared for a specific task.

Login by username / password always includes a centralised provider holding the credentials, and shifting away from that approach increases security when using the world wide web. Centralised entities storing high volumes of personal identification information are a popular target for hackers to get access to personal data. Another positive side-effect lies in a user not having to remember personal logins for each service they are using on the internet.

How is personal data processing impacted by the technology?

This is a step further on the previous use case: personal data would not be exchanged at all, as people could have a digital identity, making it safer to navigate the web and only exchanging access rights and claims to the data.

What are the main challenges raised by the use case?

The digital identity would still need to be linked to personal information outside the blockchain. If only the digital identifier is processed on the blockchain, does the technology need to comply with regulations such as GDPR? The use of hash keys in this case would be of help, as these would ensure the authenticity of the digital identity without actually transferring any personal data.

GDPR and blockchain: what you need to know

As we anticipated above, GDPR has added an additional layer of complexity to be considered in relation to blockchain technology. When personal data is processed by blockchain application, it may be replicated on a number of nodes of the ledger, and it may be stored there as long as the blockchain is operative (and possibly further, for back-up). If you consider such a statement from a GDPR perspective, this simple fact raises a number of serious questions when it comes to compliance with the regulation.

We will try in this chapter to unpack the reasons why a blockchain to process personal data would not be GDPR-compliant, and propose possible solutions on how blockchain linked to a certain way of processing personal data may be compliant with GDPR.

Who controls my data, and where is my data processed?

GDPR imposes a precise set of obligations on the controllers of personal data, i.e. the entities which determine the purposes and means of the processing of personal data. If your data is processed directly within the blockchain, then it will be replicated and distributed across the ledger, and hence physically stored in different nodes and in different locations.

Although the manager of the node might potentially use the data for a purpose other than what it was originally collected for, the very existence of the blockchain should ensure that data is not repurposed, as any activity on such data could be recorded in the chain. Potentially, there may exist a number of different controllers (or joint controllers) for the data, but practically speaking they would not have permission to re-purpose the data. The controller would be effectively the entity which either collected the data in the first place, or gave instructions to a processor to collect and process such data within the blockchain.

It is worth noting that certain regulators have tried to clarify the matter: CNIL (the French regulator) has stated that "participants, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered as data controllers. [..] More specifically, the CNIL considers that the participant is a data controller:

- when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal);
- when the said participant is a legal person and that it registers personal data on a blockchain.".

Based on the definition above, whoever registers the data in the blockchain is a controller; however not all participants in the blockchain are controllers, as the CNIL explains in its paper "Solution for the responsible use of the blockchain in the context of personal data". If we can identify the controller, we can also easily confirm whether GDPR applies to such controller (remember, it is applicable to any company based in the EU, and any companies offering services to EU-domiciled data subjects). The same is valid for other local law: for example, a controller based in Canada using blockchain technology would be subject to Canadian data protection law. As every regulation may be different, identifying the controller and where it is based plays a key role in ensuring compliance with local requirements.

The second question (where is my data processed?) may not be as easily answered. When data is processed via a blockchain, this gets replicated on different blocks, which may be physically located in non-EU countries. However under GDPR additional restrictions apply to personal data processing when this involves transfer to a third country (and the same holds for most local data protection regulations). This would also happen without the knowledge of the data subject, which would be in clear breach of the transparency principle. As a possible solution, the controller might request each node on the network to certify it is physically located in the EU, although this is difficult to control. The only way for a controller to be compliant in this case is to be transparent to the data subject and ensure that the data is safe: (i) inform the data subject of the purpose(s) of the collection and processing of personal data, (ii) inform the data subject that their data may be transferred to third countries and finally (iii) ensure (where technically possible) that appropriate safeguards are in place.

How is it ensured that my data is processed in adherence to the principles of data protection?

Let us say that I had provided my consent for my health data to be accessible to a network of doctors via a blockchain application. Different people will need to be able to access my data, but only for the purpose which I specifically consented to. For example, I may give consent to access my data for doctors to provide me with medical advice, however I do not want my data to be used for research purposes – how is the access to my data limited? Translated into GDPR terms, the structure that first collected (or which gave instructions to collect) my data is the controller, while any doctor (or better, the company they work for) that would access the data via the blockchain would be considered a processor.

A key question here rrelates to the technology itself: does every single step of the process on a blockchain have a legal basis (i.e. is it lawful)? Also, is each and every step compliant with the GDPR principles? We should remember here that for processing to be lawful under GDPR, consent is not strictly required (except in specific cases), as long as there exists another legal basis for processing (e.g. there is a contractual necessity for processing the personal data). This may not be true under different data protection regulations.

A way to at least partially control this mechanism would be to ensure that any organisation participating in the network would sign a data transfer agreement confirming the data will not be re-purposed. The blockchain should then allow access to the data only to parties who have signed the agreement, and should make the data accessible only in connection with the original consent form, so that anyone accessing it would be aware of the purposes for which the data can be used. The blockchain would then serve the purpose of validating the credentials of people accessing the data, and could also be a way to limit the use of such data (e.g. data can only be accessed, but not sent outside the blockchain network, unless for the specific purposes (and via the specific means, e.g. a certain software) authorised by the data subject.

This solution would ensure that data is used only for specific purposes, without the need for the data subject to provide consent for any party which would need access to their record.

Is my data secure against breaches?

Blockchain are often regarded as one of the safest method to transfer and share pieces of information, and we will not question that in this chapter. However, regardless of how safe the system is, there is always the possibility of a breach, and however small this might be. GDPR requires certain breaches to be notified to the supervisory authority within 72 hours. Tthe question here is: if a node of the blockchain is compromised, whose responsibility is it to ensure timely reporting to the authority? As the data is distributed, the controller might even not be aware of a breach at one of the nodes.

For this reason, it is crucial that any node administrator is aware of its responsibility and notifies the controller as soon as any breach occurs. it is also a responsibility of the controller to ensure that any processor (i.e. any node administrator) is aware of its obligations, so that any party entering a blockchain should be made aware (by the controller) of its obligations in regards to data breaches. Awareness can be ensured by means of standard clauses to be signed by any participant in the block chain, where the participant is required to explicitly acknowledge such clauses.

How can I exercise my rights on a blockchain? Can I be forgotten?

Under GDPR a number of rights are guaranteed to data subjects. Certain rights might be facilitated by the use of blockchain (e.g. compliance with access rights might be easier, given the structured nature of data normally processed in such systems). Other rights can raise challenges to the controller of data being processed on a blockchain. To start with something relatively simple, if I object to the processing of my data, or otherwise withdraw consent for my data to be processed, how will it work? Any piece of data is recorded in the chain and used in subsequent steps for validation purposes – we cannot simply ask the system to stop processing certain data collected in a number of nodes. Note that, even if the data is no longer actually used, its storage in the network is considered as processing under GDPR.

Let us move to a critical right under GDPR: “the right to be forgotten”. Assume that I have provided consent for my financial data to be processed on a blockchain at a time when I was looking for a mortgage, so that different banks could access my records and provide me with their best offer. I am no longer looking for a mortgage, so I want to make sure that such data is now deleted from the system: is this even possible? As the data is stored in a number of different nodes, and should not be tampered with, how can it be deleted? It seems that the answer lies in how the blockchain is set up in the first place, because when personal data is effectively distributed across the ledger, there is no way one could delete the data from each node. You could block access to it, but it would still be there and, as such, potentially available for someone to use. Also, anonymisation would not be an option here, as the blockchain would not allow any kind of tampering with the original data.

When the blockchain is used to store or transfer personal data in any form, the record of that data could never be deleted from the chain. If the controller decides to use the blockchain for this purpose, it should at the very least pre-emptively inform the data subject that their data will never be deleted, and that by using the network they are implicitly renouncing to the right to be forgotten. GDPR does not account for such a possibility, hence this would actually be in breach of a direct requirement under the regulation. This type of use cases calls for a change in the regulation to take into account the existence of a technology that simply does not allow erasure of data: at the very least, we hope that these situations will be addressed in the upcoming ePrivacy regulation.

Until the regulation becomes more flexible to account for these type of technology, the way to be compliant (i.e. the way for the right of erasure to exist on a blockchain) is to not use the blockchain to store or transfer any personal data at all. We explain this approach in the next chapter.

The smarter way for blockchains

A common misconception (and misuse) of a blockchain is that it can be leveraged to store information. In reality, blockchains are a very expensive and inefficient way to store (and process) data. This is simply because anything that goes in the blockchain is replicated in different nodes, which translates into having to use more storage space (and computational power) that you would need with more traditional technology.

If companies want to leverage blockchain technology in a smart and cost effective way, they should consider using the blockchain only as a mean to verify that certain data exists outside the chain, rather than storing/transmitting the actual data via the chain.

Concretely, this can be achieved by the use of hash keys in the blockchain, which refer to data stored in an external database. Following this approach, personal data would be stored in a database not connected to the blockchain, while any individual to which such data belongs would be identifiable in the blockchain by means of a hash key. This would result in a more efficient way to use the new technology, and it would also make compliance with GDPR easier to achieve: personal data would be stored in one physical place, and as long as the hash key does not carry any information to identify the data subject, it can be stored in nodes all over the world without any consequence for compliance with data protection requirements.

Using blockchain in this way would solve most of the problems described above: the right of erasure could be achieved by deleting the data outside the chain (without changing the hash key itself), the data controller would be easily identifiable as the data does not leave the place where it is stored in the first place, and data breaches would be easier to manage (only breaches to the database where the personal data is physically stored would need to be reported). Essentially, this allows the use of the technology without having to ensure that the blockchain itself is compliant with GDPR.

What's next?

GDPR is a regulation strictly focused on "traditional means" for processing personal data. When it comes to data processed in a network, shared with a number of users, and flowing seamlessly across borders, it falls short in providing clear answers to the question how can this technology be compliant with the requirements.

While GDPR is clearly not technology-oriented, the upcoming ePrivacy regulation promises to be "future-proof", and as such applicable to any electronic means for the processing of personal data. As the text is not final yet, it is hard to provide an assessment of such promise, but it is sensible to assume that the new requirements may provide additional answers to the questions raised above. If you want to know more about ePrivacy, you can read our publication "Is ePrivacy defining the future standard of data protection for the banking industry?".

All in all, we want to stress – one last time – that, unless the regulatory framework evolves to account for this technology, processing of personal data directly on a blockchain is currently non-compliant with the EU data protection regulation.

How can PwC help?

As a multi-disciplinary practice, we are uniquely placed to help our clients adjust to the new environment. Our data protection team includes lawyers, consultants, cybersecurity specialists, auditors, risk specialists, forensics experts and strategists. Our global team of experienced business, technology and regulatory leaders can help you identify how blockchain can benefit your organisation and how to rapidly move your initiatives forward

Our team is truly global, proposing innovative solutions with on the ground expertise in all the major EU economies.

Thanks to our extensive expertise in both blockchain technology and data protection matters, we can help you in implementing the best solution for your business. Starting from the assessment of your current situation, we determine whether blockchain is effectively the most appropriate technology for your needs and design it in line with the GDPR principle of “privacy by design and by default”, to ensure compliance with the regulation – always keeping in mind the economic and compliance constraints of processing personal data directly on a blockchain.

Assessment of status quo
Market assessment and identification of your priority needs (e.g. make transfer of personal data more secure, ensure data is correct, make validation processes more efficient, etc.).

Solution design
Identify the technology that best answer your needs. In this phase, we help you apply from the very beginning the principle of data protection by design and by default, to ensure the solution is fully compliant with GDPR. We can also support the data protection impact assessment required under GDPR when new technologies are implemented for the processing of personal data.

Implementation
We can work with you to implement the designed solution and ensure that the final technology answers to all of your needs identified in the first step. Our data protection expertise will help you determine that the implemented solution meets the GDPR requirements.

Handover to Business as Usual
The critical part of any project is the handover to BAU, and we can support you all the way to completion of the handover to ensure your staff is fully trained and capable to run the designed processes.

For additional information, please contact our experts:

Patrick Akiki
PwC, Partner
Office: +41 58 792 25 19
Mobile: +41 79 708 11 07
akiki.patrick@ch.pwc.com

Morris Naqib
PwC, Senior Manager
Office: +41 58 792 42 83
Mobile: +41 79 902 31 45
morris.naqib@ch.pwc.com

Mark Hussey
PwC, Senior Manager
Office: +41 58 792 45 52
Mobile: +41 79 549 07 59
mark.hussey@ch.pwc.com

Isabella Sorace
PwC, Manager
Office: +41 58 792 28 29
Mobile: +41 79 742 37 16
isabella.sorace@ch.pwc.com

Pierre-Edouard Wahl
PwC, Director
Office: +41 58 792 16 33
Mobile: +41 79 346 44 98
pierre-edouard.wahl@ch.pwc.com

Key contributors:
We would like to thank Jutta-Sonia Oberlin and Denise del Pozzo Silva for their valuable contribution to this publication.

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00