DIGITALISATION

APRIL. 2023

Renting instead of buying - but how secure is the user data?

An article of the Swiss Association of MBAs

CRISTIAN MANGANIELLO
Author

Sharing offerings are also gaining ground in the business-to-business sector. More and more frequently, companies are renting products as a comprehensive, data-based service package instead of buying them. Landlords, tenants and users have a common interest in ensuring that the user data collected, which is often personal in nature, is processed and stored securely. This assurance is provided by an independent assurance engagement.

Shared use is a win-win all round

Driven by the trend towards renting instead of buying and the advent of the Internet of Things, a powerful sharing economy has emerged spanning almost every industry, from taxi services and washing machines to financing solutions. What has been the norm for end customers for quite some time is now also gaining acceptance in the business world, replacing traditional operational leasing. Understandably so, because if a company purchases a product as a service package on a temporary basis, it makes its costs more flexible, reduces tied-up capital and automatically keeps up to date with the latest technology and techniques. From the manufacturer's perspective, this changes the business model from being a pure manufacturer to a service provider (also known as 'servitisation').

Two examples from practice

Example 1: A manufacturer of machine tools makes its products available to construction companies and craft businesses as a rental solution with an integrated maintenance contract. Thanks to the way the portfolio is digitally networked, it always knows where and when a machine is in use and how long for. This enables the manufacturer to accurately predict the maintenance requirements of their tools and inform their customers in good time. When the tools are developed in this way, they remain in use for longer and can make a significant contribution towards sustainability.

Example 2: A pharmaceutical company offers customised analysis platforms. Here, hospitals, clinics or medical professionals can use algorithms and artificial intelligence to transform their operational data or diagnoses into insights into services, treatments and therapies, thereby optimising their operational efficiency and patient care. In this example, the payment method changes to 'pay-per-use' or 'pay-per-analysis' in addition to the use of data.

Data as a product

Business models with digital services are based on a valuable raw material: data. The providers of these types of services usually collect extensive and, where necessary, personalised information.

They know who uses their service in which company, when and to what extent. They can use this to draw conclusions about consumption, consumption patterns, individual teams or even people. This raises a big question for everyone involved in the business model, i.e. for landlords, tenants and users: how secure is this data?

This raises a big question for everyone involved in the business model, i.e. for landlords, tenants and users: how secure is this data?

Corporate responsibility reloaded

The possession and use of personal data implies that it must be protected accordingly. Both the machine tool manufacturer and the analytics platform provider from our examples above must provide transparency about the security and use of collected data and make sure it meets legal, regulatory and contractual requirements, and is processed and stored in accordance with applicable rules. For example, they must comply with the European Union's General Data Protection Regulation (EU GDPR) or the Swiss Federal Act on Data Protection and its Ordinance (FADP and DPO), its counterparts in Switzerland.

Regulated customers or customers with a high level of maturity in particular often demand more than just confirmation that the requirements are being met. They demand that an independent practitioner validates this confirmation and provide an assurance report. This is done with the aim of achieving control over their upstream and downstream value creation processes. This is where independent testing based on an internationally recognised standard comes into play.

Review of secure data processing and storage

The review of information security in certain lines of service is voluntary, i.e. there's no explicit legal mandate for it. After all, in most cases the data is non-financial. As an independent practitioner, we therefore

THE REVIEW OF INFORMATION SECURITY IN CERTAIN LINES OF SERVICE IS VOLUNTARY, I.E. THERE'S NO EXPLICIT LEGAL MANDATE FOR IT.

apply auditing standards for non-financial reporting.

- In an international context, ISAE 3000 (Revised), which was updated by the International Auditing and Assurance Standards Board (IAASB) in 2013, is suitable for this purpose. The standard is principle-based and can be applied to a wide range of non-financial audit engagements, such as statements on corporate social or digital responsibility, data security or internal control systems.
- If a company primarily operates in the United States, a Service Organisation Control (SOC) review is a good choice. A SOC-2® report takes a close look at internal controls related to security, availability, integrity and confidentiality (data protection) – the so-called Trust Services Criteria – with the security criterion being mandatory.

A good idea, all things considered

An assurance engagement provides very attractive benefits. The report provides assurance to the audited entity that it is compliant with the contractual terms and conditions, as well as the provisions of the regulator, the standard setter and self-regulator in all relevant areas. The company can demonstrate compliance with defined requirements to its stakeholders through the review and report by an independent practitioner. The initial effort required to develop the criteria is considerable and, as in the case of statutory audits, operating as well as costs for the assurance engagement incur. But depending on the situation regarding the contract, the company may be able to pass on these costs and/or benefit from them for a number of years.

Opportunity rather than a necessary evil

The law doesn't require an independent assurance engagement. So, for once, it isn't a necessary evil, but instead a promising opportunity or a means of differentiation. Companies that provide or use digital services instead of or with products should ask themselves whether those services are secure, and whether they have maximum transparency of the risks associated with the data involved. Proving that this is the case not only strengthens companies' compliance but can also be used as a real competitive advantage and a vote of confidence.

With an ever-increasing need for more security and transparency, consumers and stakeholders alike require more and more visibility in storage and processing of their data.

As such, it is inevitable for a company to not only implement adequate risk management procedures but having the effectiveness of such controls attested by an independent third party that can issue such an attestation for the broader audience.

With an ever-increasing need for more security and transparency, consumers and stakeholders alike require more and more visibility in storage and processing of their data.

About the Author

Cristian Manganiello is a Partner at PwC Switzerland within the Digital Assurance practice, where he started his career in 1999. He has a strong background in financial accounting and auditing, with significant experience in the end-user aspects of information systems consulting. His extensive experience spans several industries, including retail, public administration, consumer goods, pharmaceuticals, life sciences and pension funds.