

GDPR v praxi – příprava a zavádění

ne slova, ale konkrétní kroky

Tomáš Hlavsa

Atos

1 Právní analýza

2 Revize procesů

3 Datový audit

4 Report a návrh nápravných opatření

5 Zavádění opatření

1 Právní analýza

GDPR - eIDAS

Právní analýza by ruku v ruce měla jít s analýzou rizik.

Proč?

Deklarace souladu s legislativou prostřednictvím zpracované ale **nezavedené** bezpečnostní politiky v organizace je bohužel častým jevem

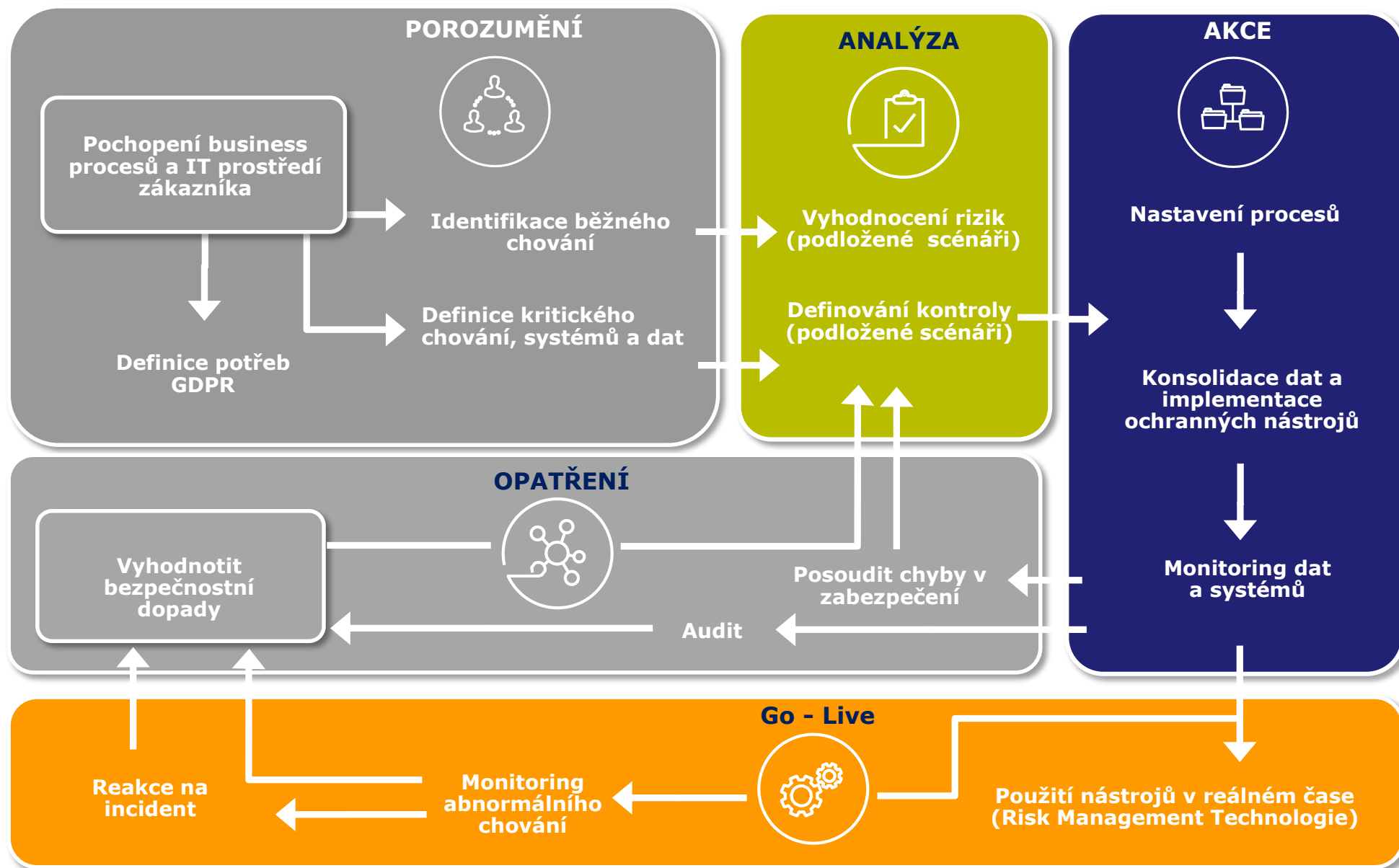
#	Požadavek	Ano	Ne	Částečně
1	Je zabezpečena ochrana perimetru Firewalllem?	X		
2	Je zpracovaný akt formou směrnice stran řízení přístupu k informačním systémům?	X		
3	Máte vytvořenu politiku klasifikace dokumentů?	X		

V POHODĚ?

2

Revize procesů

Procesní schéma ověření dopadů GDPR do procesů a systémů



3

Datový audit

Hodnocení rizik GDPR dat

5 jednoduchých otázek

1. Jaká osobní data občanů EU máte v držení?
2. Jak citlivá data to jsou?
3. Kde se v rámci organizace tato nacházejí a kdo k nim přistupuje?
4. Jak se v organizaci pohybují, kam a kudy z organizace odcházejí?
5. Jak se s nimi pracuje a komu jsou poskytována?

Fáze 1 - Analýza statických dat

Poznejte, kde jsou uložena Vaše osobní data

Tato analýza zahrnuje zjištění, detekování osobních dat občanů EU napříč Vaší datovou infrastrukturou, tedy síťovými úložišti, databázemi a cloudovými úložišti. Naše platforma má vestavěné politiky detekující datové vzory GDPR, nemusíte je tedy složitě definovat. Vlastní vzory GDPR dat typické pro Vaši organizaci Vám rádi nastavíme a budeme schopni detekovat jejich přítomnost jak na lokálních, síťových i cloudových úložištích.

Naše platforma „ATOS threat aware data protection“ skenuje úložiště, která určíte za účelem identifikace:

- Všech typů osobních dat
- Úrovní citlivosti těchto dat
- Která úložiště obsahují osobní data



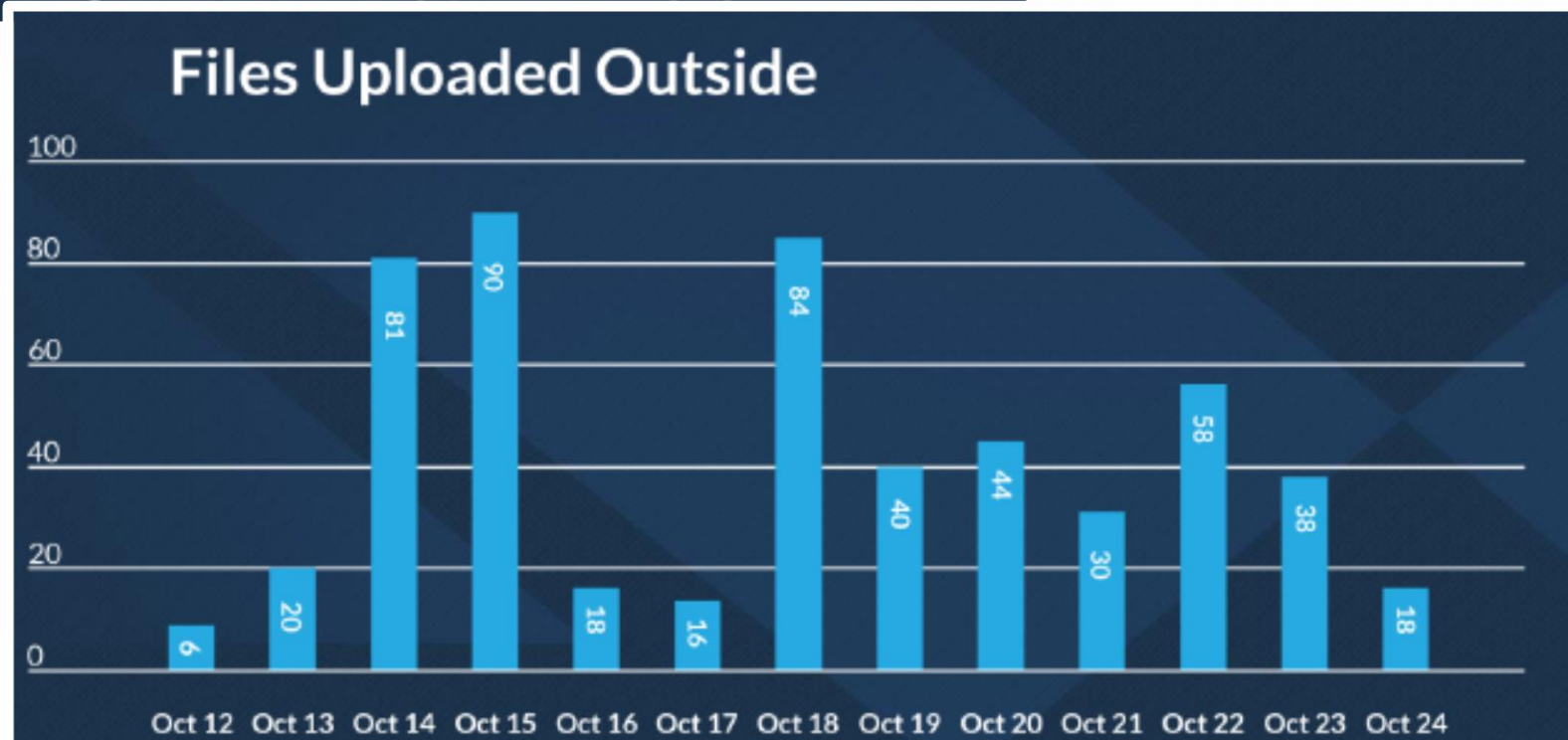
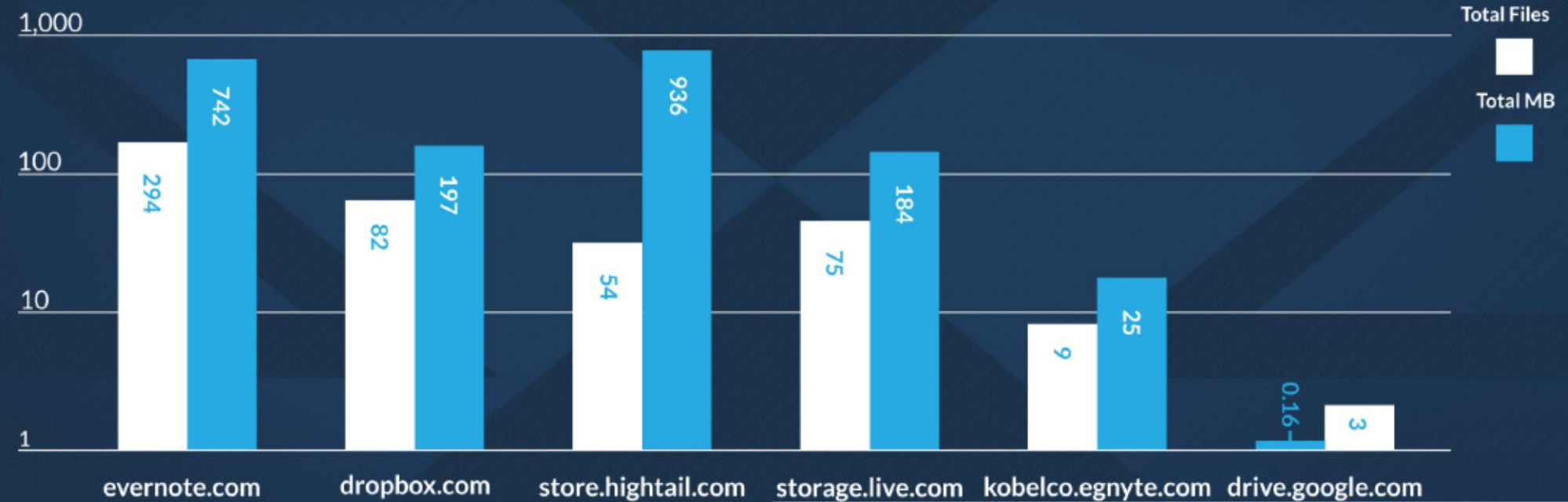
Fáze 2 - Analýza dat v pohybu

Zmapujte pohyb osobních dat

Tato analýza identifikuje jak se GDPR data pohybují uvnitř Vaší organizace a jakými cestami Vaši organizaci opouštějí. Naše platforma používá stejné datové vzory jako při analýze statických dat a to za účelem identifikace:

Všech typů osobních dat v pohybu

- Úrovně citlivostí těchto dat v pohybu
- Zdroj a cíl, tedy odkud a kam jsou osobní data přenášena
- Kanály, kterými osobní data opouštějí Vaši organizaci, např. web, email....



Fáze 3 - Report a doporučení

Připravte se na nápravná opatření

Jakmile jsou obě analýzy (statická data a data v pohybu) dokončeny, poskytne Vám Atos náhled na Vaše GDPR data který potřebujete k rozhodnutí, kde jsou rizika největší a jaké by měly být Vaše další kroky. Tento náhled ve formě reportu v sobě zahrnuje:

- Ucelený přehled rizik
- Detailní report analýzy dat
- Přehled zjištění
- Doporučení **strategie** nápravných opatření

4

Report a návrh nápravných
opatření

Fáze 3 - Report

Detailní popisy

Atos

Data of Interest Definition

Policies are an important aspect of the data exposure assessment. Policies determine the data patterns that are of interest and that are potentially sensitive, as well as 'out of the box' policies.

Atos

Introduction

This data exposure assessment report has been produced by Digital Question for <Customer Name> following the completion of the data analysis tasks performed on premise at <Customer Name> data centers located in <location> and <location>.

The report contains a detailed analysis of <Customer Name> storage repositories using policies agreed with <Customer Name>. <Customer Name> identified a number of data assets that they wished to be audited. Only incidents were generated during the assessment.

The data exposure assessment has provided visibility of sensitive data across multiple channels including Email, Web and storage repositories. During the assessment a number of 'significant' violations have been escalated to <Customer Name>. These incidents would pose a severe impact on the reputation of <Customer Name> and possible financial loss should they continue to occur.

Assessment Scope

<Customer Name> chose to audit email and web traffic crossing the corporate boundary in <location> and <location>. <Customer Name> also chose to audit data repositories to identify the potential presence of sensitive data. Email and web protection policies were configured to only monitor traffic, and the system was configured to not store any file attachments contained in outbound email communications or web postings. Traffic was monitored for 30 day period.

The discovery identification policies were configured to not store any artifacts relating to any identified files. All data repositories were scanned in single pass.

Data Repositories

Detailed below are the data repositories that were identified by <Customer Name>.

Repository Name	Location	Access Method
Network Share	192.168.1.100	\\192.168.1.100\share
SQL Server	192.168.1.101	sql2012.demosql.com
OneDrive for Business	192.168.1.102	demo1ab-my.sharepoint.com

Network Communication Monitoring

Digital Question's email and web protection modules were enabled and activated. All outbound corporate email was monitored as part of the assessment. The web protection module was integrated into <Customer Name>'s existing web security proxy appliance, squid.demosql.com, which was identified as a squid proxy server.

Email Configuration

<Customer Name> uses both on-premise email solution, Exchange 2013, and an Office 365 tenancy. Two email modules were enabled, one to process outbound on-premise traffic and one to process outbound email originating from the cloud service. Once processed all outbound email was then delivered only to the corporate SMTP, 192.168.1.103, for onward delivery to the intended recipient.

Web Configuration

All inbound web traffic traverses a squid proxy server, squid.demosql.com. The squid proxy server was configured to audit all web traffic to the Digital Question's DAP service, where all logs were scanned. All logging of logs was configured.

Proprietary and Confidential

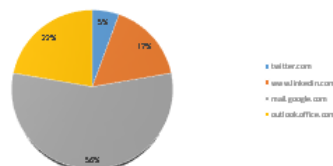
Datový audit

Atos

Top Policies by Protocol

Atos

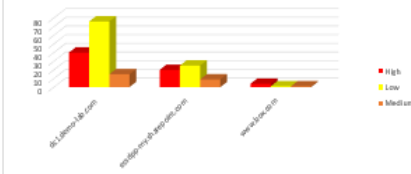
Web Incidents by Destination Web Host



Corporate data has been detected within web transactions. Over 50% of all incidents were internal users sending data to [mail.google.com](#). This included PII and PHI data, which can result in large financial penalties.

Data Repository

Discovery Incident Severity Breakdown by Repository



The data at rest is can have identified a range of incidents on all repositories scanned. Internal file shares have highly confidential information stored on them, as do the corporate OneDrive for Business and Box accounts. The cloud storage potentially be shared with external parties and should be removed as soon as possible.

Proprietary and Confidential

Doporučení

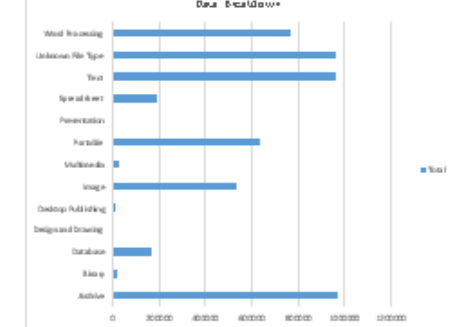
Atos

Conclusion and Recommendation

Atos

6 out of 625 the corporate data matching each case pattern, of which a large proportion of these the corporate data is in 10 business critical case patterns. The corporate data was made available to the scanning engine and the data was scanned with a data protection or encryption policy, as part of the assessment to ensure the data is secure. During policy scanning the data was scanned with a data protection or encryption policy, as part of the assessment to ensure the data is secure. The data was scanned with a data protection or encryption policy, as part of the assessment to ensure the data is secure. There were many instances of the corporate data being scanned.

Discovery of data within the corporate data repository is a significant finding. The data was scanned with a data protection or encryption policy, as part of the assessment to ensure the data is secure. The data was scanned with a data protection or encryption policy, as part of the assessment to ensure the data is secure. The data was scanned with a data protection or encryption policy, as part of the assessment to ensure the data is secure.



Proprietary and Confidential

Atos

5 základních otázek – pamatujete?

Otázka	Výstup v reportu
1. Jaká osobní data občanů EU máte v držení?	Detailní popis, kde se data obsahující osobní údaje nacházejí vč. rozložení po jednotlivých zdrojích.
2. Jak citlivá data to jsou?	Popis způsobů vč. četnosti, jak osobní údaje opouštějí Vaši organizaci.
3. Kde přesně v rámci organizace se tato nacházejí?	Detailní popis úložišť obsahujících osobní data.
4. Jak se v rámci organizace pohybují a kam a jakými kanály z organizace odcházejí?	Real-time a historický pohled na osobní data opouštějící Vaši organizaci umožní detekovat a notifikovat o potenciálním úniku osobních dat.
5. Jak se s nimi pracuje a komu jsou poskytována?	Doporučení politik, architektury a životního cyklu dokumentů k zajištění vyšší úrovně ochrany.

5

Zavádění nápravných opatření

— ATOS program ochrany GDPR dat

Vyhodnocení
rizik GDPR dat

PoznejTe, kde máte uložena osobní data, jak je s nimi nakládáno, která data jsou ta nejcitlivější a požadujete pro ně vyšší ochranu.

Automatizace
klasifikace
všech osobních
dat

Zautomatizujte klasifikaci Vašich osobních dat s důrazem na zdroje a jejich kontrolu

Zabezpečení
ochrany dat

Používejte technologie jako je DLP, Identity Access Management a šifrování

Úprava
plánu zvládní
incidentů

Zaktualizujte si své plány zvládní detekovaných incidentů abyste byli na podobné situace připraveni

Demontrace
souladu s
GDPR

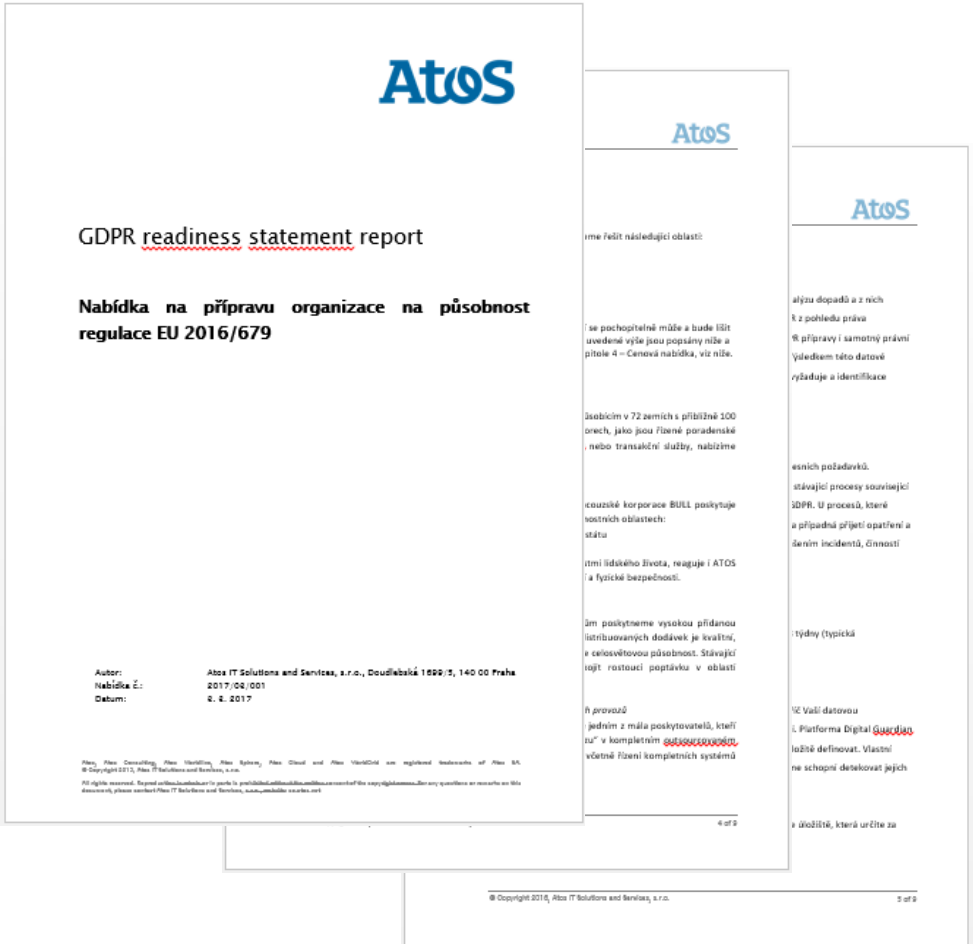
Použijte své analýzy a jejich výstupy k předvedení svého souladu s požadavky GDPR

A close-up, slightly blurred image of a clock face. The clock has a white face with black numbers and hands. A red second hand is visible, pointing towards the 12. The background is a soft, out-of-focus grey.

KDY ZAČNETE?

HNED?

ZAČNĚTE HNED !!



č.	Položka	Cena v Kč bez DPH
4.1	Právní analýza v rozsahu 4 člověkodnů	98 500 Kč
4.2	Procesní analýza v rozsahu 7 člověkodnů	112 250 Kč
4.3	Datový audit v rozsahu 2-3 týdnů vč. přípravy	64 100 Kč
4.4	Příprava role DPO v rozsahu 3 člověkodnů	75 600 Kč
4.5	Vyhotovení GDPR <u>readiness statement</u> reportu v rozsahu 2 dnů na základě předchozích analýz	30 430 Kč
	Celkem	380 880 Kč

Atos

Trusted partner for your Digital Journey