Die Neue Datenschutz-Grundverordnung, vom Fachmann erklärt: Chancen inmitten des Chaos

O novo Regime Geral de Proteção de Dados explicado pelo especialista: Encontrar oportunidades no meio do caos

RICARDO PINTO

Die meisten Leser dieses Artikels werden wissen, dass am 4. Mai 2016 die Europäische Union in ihrem Amtsblatt eine neue Verordnung für den Datenschutz der Bürger der Europäischen Gemeinschaft (EG) veröffentlicht hat. Diese Verordnung ist 20 Tage danach in Kraft getreten, mit einer Übergangszeit von 2 Jahren, damit sich Unternehmen und Organisationen an die neuen Anforderungen anpassen können, bevor sie dann am 25. Mai 2018 unmittelbar gelten werden.

Das Thema ist eigentlich nicht neu: Datenschutzgesetze gibt es bereits in allen EU-Ländern, doch allein der Umstand, dass 28 unterschiedliche Gesetzgebungen im europäischen Rahmen aufeinandertreffen, trägt weder zur Entwicklung eines gemeinsamen Geschäftsstandards bei, noch dazu, dass Dateninhaber überall ihre Rechte wahrnehmen können.

Im Vergleich zur bestehenden Gesetzgebung gibt es spürbare Änderungen, die für diejenigen noch einschneidender erscheinen, die jetzt mit der Datenschutz-Grundverordnung (DSGVO) erstmals in Kontakt treten, ohne die Leitlinien des derzeitigen (noch geltenden) Datenschutzgesetzes (67/98) zu kennen. Viele der Pflichten, die das Datenschutzgesetz auferlegt, sind in der DSGVO gleichgeblieben, doch gibt es auch neue Themenfelder, die einer dringenden Handlung bedürfen. Und dies umso mehr, als dass die neue ***ePrivacy*-Verordnung** (welche die DSGVO mit Hauptaugenmerk auf elektronische Kommunikationen ergänzt) die Grundlinien ihres medienwirksameren "großen Bruders" noch verstärkt.

Ich werde mich an dieser Stelle auf drei regulatorische Maßnahmen beschränken, um dann eine Brücke zu den **Kollateralnutzen der Verordnung** zu schlagen:

- **Die Sicherheit** der Personendaten: Die Verordnung verpflichtet, dass sowohl der für die Verarbeitung Verantwortliche (*Data Controller*) als auch der Auftragsverarbeiter (*Data Processor*) die angemessenen **technischen und organisatorischen Maßnahmen** ergreift, um ein sachgemäßes **Sicherheitsniveau zu gewährleisten.** Diese Maßnahmen gehen vom Einsatz der Pseudonymisierung und Verschlüsselung der Daten, bis hin zum Nachweis der Fähigkeit, die 4 Prinzipien der Informationssicherheit sicherzustellen: Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
- **Prozesse,** die es dem Verarbeitungsverantwortlichen und dem Auftragsverarbeiter ermöglichen, regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitungssicherheit zu testen, sollen einzuschätzen und zu bewerten sein.
- **Auftragsverarbeiter** (einer der Eckpfeiler der DSGVO) werden nun direkte Pflichten und Verantwortlichkeiten haben,

Será do conhecimento da maioria dos leitores deste artigo que no dia 4 de maio de 2016 a União Europeia publicou no seu jornal oficial um novo regulamento para a protecção de dados dos cidadãos da comunidade europeia (CE). Este regulamento entrou em vigor 20 dias depois, com um período de transição de dois anos, para que organismos e organizações se ajustem às suas exigências, entrando em cumprimento no dia 25 de maio de 2018.

O tema não é novo, existem leis de protecção de dados nos países da CE, mas o simples facto de 28 legislações diferentes concorrerem entre si num contexto de ecossistema europeu, não contribui para o desenvolvimento de um standard de negócio nem para a possibilidade de exercício dos direitos dos titulares dos dados.

Assim, havendo mudanças sensíveis face à legislação existente, estas são mais críticas para quem esteja a tomar contacto com o Regulamento Geral de Protecção de Dados (RGPD) desconhecendo as directrizes da actual (e em vigor) Lei de Protecção de Dados (67/98). Muitas das obrigações que a lei de Protecção de Dados impõe mantêm-se no RGPD, mas há tópicos novos que trazem a necessidade de acção urgente. Mais ainda porque o novo **regulamento *ePrivacy*** (complementa o RGPD com foco nas comunicações electrónicas) reforça as directrizes mestras do seu "irmão" mais mediático.

Como certamente já terão conhecimento das principais obrigações do RGPD, foco-me em três das medidas regulamentares para fazer a ponte para os **benefícios colaterais do regulamento**:

- **Segurança** dos dados pessoais. O regulamento obriga a que, quer o responsável pelo tratamento (*Data Controller*) quer o subcontratante (*Data Processor*) apliquem **medidas técnicas e organizativas** adequadas para assegurar um **nível de segurança adequado.** As medidas vão desde o uso de pseudonimização e encriptação de dados, à demonstração da capacidade de assegurar os 4 princípios da segurança de informação: Confidencialidade, Integridade e Disponibilidade + Resiliência
- **Processos** que permitam ao responsável tratamento e subcontratante(s) testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
- **Subcontratantes** (uma das pedras de toque do RGPD) terão obrigações e responsabilidade directas, o que significa que podem ser directamente responsabilizados por quaisquer violações de dados. A responsabilidade fica contratualizada (entre subcontratante e responsável pelo tratamento), documentando o objeto e duração do tratamento, a natureza e fi-

"Viele der Pflichten, die das Datenschutzgesetz auferlegt, sind von der DSGVO direkt übernommen worden, doch gibt es auch neue Themenfelder, die einer dringenden Handlung bedürfen."

"Muitas das obrigações que a lei de Protecção de Dados impõe mantêm-se no RGPD, mas há tópicos novos que trazem a necessidade de acção urgente."

Ricardo Pinto

was bedeutet, dass sie direkt für jegliche Datenverletzungen haftbar gemacht werden können. Die Verantwortung wird vertraglich (zwischen dem Auftragsverarbeiter und dem Verarbeitungsverantwortlichen) geregelt, womit der Gegenstand und die Dauer der Verarbeitung, die Natur und der Zweck, die Arten von Personendaten und Personenkategorien, die Pflichten und Rechte des Verarbeitungsverantwortlichen dokumentiert werden. *(H.d.A.: damit werden, alle Beteiligten des Systems, namentlich die Unternehmer, für die Einhaltung der DSGVO zur Verantwortung gezogen).*

Betrachtet man ganzheitlich die 99 Artikel der DSGVO, so dreht sich alles um einen Grundsatz: ***Accountability*** oder **Rechenschaftspflicht.**

Nun könnten wir uns zu folgender Frage verleiten lassen: Können wir nach mehr als 30 Jahren eines unaufhaltsamen Vormarsches der Technologie, ausgehend vom Lochpapier und Kellern voller Aktenordner bis hin zum Einsatz der *Cloud, Big Data* und *IoT*, noch die Kenntnis aller Daten garantieren, die wir in unseren (persönlichen, geschäftlichen, finanziellen, etc.) Organisationen erheben, erzeugen und verarbeiten? Sind wir noch in der Lage, folgende Fragen beantworten?

1. Welche personenbezogenen Daten erheben und speichern wir in unseren Organisationen?
2. Warum brauchen wir sie überhaupt?
3. Wie lange müssen sie in unserem Besitz bleiben?
4. Wo werden sie gespeichert? An welchen Orten (einschließlich Backups, Test- und Entwicklungsumfelder)?
5. Wer hat Zugriff auf diese Daten? Müssen wirklich alle Zugang haben?

Die Antworten werfen unweigerlich eine Reihe von Zweifeln auf, deren Klärung als Ausgangspunkt für die notwendigen Initiativen zum Erreichen der Verordnungskonformität dienen. Diese potentiell schmerzliche Übung ist zweifelsohne wesentlich, angesichts der bevorstehenden Herausforderungen, und keine Technologie kann sie uns abnehmen (sondern bestenfalls dabei helfen). Die guten Nachrichten finden sich jedoch ein, wenn wir anschließend die Resultate analysieren, namentlich durch die Identifizierung von:

- Personendaten, die wir nicht mehr brauchen;
- "*shadow* IT": Ausrüstungen und selbst Komplettlösungen, die noch weiterbestehen und in der Vergangenheit geschaffen wurden, um auf gelegentliche Anforderungen zu reagieren, dann aber nicht weitergeführt wurden oder nie ihre Funktion erfüllt haben, und in denen hingegen immer noch (Personen- und Geschäfts-). Daten gespeichert sind;
- denjenigen Mitarbeitern, die tatsächlich Zugriff auf Personendaten brauchen, und welches die entsprechenden Verarbeitungsprozesse sind;
- Ineffizienzen von Software-Lizenzverträgen;
- Ineffizienzen bei der Nutzung von Datenspeicherplatz gegenüber den wirklichen Erfordernissen (dies kommt dem neuen Grundsatz der Datenminimierung entgegen);
- anfälligen, für die IT-Verwalter "unsichtbaren" Geräten.

Neue Geschäftschancen bringen Veränderungen mit sich, nicht selten verbunden mit der Eingliederung neuer Technologien (damit einhergehend neue Risiken der CyberSecurity), die wenn sie nicht sachgemäß geschützt werden, Angriffsflächen für Cyber-Bedrohungen wie *Ransomware* oder Industriespionage bieten (z. B. durch eingenistete *Advanced Persistent Threats*). Somit bilden die Einführung von Best-Pratice der Firmen-IT und Informationssicherheit mehr denn je einen Mehrwert.

nalidade, os tipos de dados pessoais e categorias dos titulares, as obrigações e direitos do responsável pelo tratamento. *(NdA: forma de corresponsabilizar os intervenientes do ecossistema, nomeadamente o industrial/empresarial no cumprimento do RGPD).*

Olhando de forma holística para os 99 artigos do RGPD, o seu foco recai sobre um princípio: ***Accountability*** ou **Responsabilização.**

Podemos sentir-nos tentados a perguntar: após mais de 30 anos de uma inexorável caminhada da tecnologia, partindo do papel caneta e caves de dossiers, até à adopção da *Cloud, Big Data* e *IoT,* será que podemos garantir conhecimento dos dados que recolhemos, produzimos e processamos nas nossas organizações (pessoais, negócio, financeiros, etc.)? Sabemos a responder a:

1. Que dados pessoais recolhemos e guardamos na nossa organização?
2. Porque precisamos deles?
3. Durante quanto tempo necessitamos de os ter na nossa posse?
4. Onde estão guardados? Em que locais (incluindo backups, ambientes teste e desenvolvimento)?
5. Quem tem acesso a estes dados? Todos precisam de ter acesso?

As respostas levam necessariamente a um conjunto colateral de dúvidas cujo esclarecimento serve de ponto de partida para as iniciativas necessárias à obtenção da conformidade regulamentar. Sendo um exercício potencialmente doloroso, é sem dúvida fundamental face aos desafios, e nenhuma tecnologia o pode fazer (no limite pode ajudar). No entanto, as boas notícias chegam quando analisamos os resultados, nomeadamente pela identificação de:

- dados pessoais que já não necessitamos;
- "*shadow* IT", equipamentos e mesmo soluções completas que subsistem e que foram criadas no passado para responder a necessidades ocasionais, que foram depois descontinuadas ou nunca chegaram a cumprir a sua função, mas que armazenam dados (pessoais e de negócio);
- que colaboradores têm efectivamente necessidade de acesso a dados pessoais, e quais os respectivos processos de processamento;
- ineficiências no licenciamento de software;
- ineficiência na utilização de armazenamento de dados face às reais necessidades (vai de acordo ao novo princípio da minimização dados);
- equipamentos vulneráveis "invisíveis" aos administradores de TI;

Was hat aber die CyberSecurity mit der DSGVO zu tun?

Wie ich zu Anfang des Artikels ausführte, zwingt die Konformität mit der DSGVO Unternehmen dazu, angemessene **Sicherheitsmaßnahmen für Personen, Prozesse und Technologie** zu ergreifen. Diese Maßnahmen haben einen Mehrwert, denn sie führen infolge einer Beratung über neue Prozesse, Weiterbildung / Schulung der Mitarbeiter, sowie neuer Technologie (in Maßen), zu einem Wandel der Unternehmenskultur, zur Rechenschaft eines jeden einzelnen Mitarbeiters für seine Aufgabe und zu neuen Chancen, wie es Sun Tzu in seinem Werk Art of War so treffend beschrieb: *„In the midst of chaos there is also opportunity".*

Hierzu nenne ich ein paar Beispiele:

1. *Compliance is the new sexy*

Die Einhaltung gesetzlicher Bestimmungen wird auf natürliche Weise ein Hebelfaktor für neue Geschäfte, Partnerschaften und Investitionen mit ebenfalls konformen Organisationen sein, die nur eine Zusammenarbeit unter Gleichen zulassen werden. Der Datenschutz ist bereits ein Unterscheidungsmerkmal für Online-Aktivitäten in allen Geschäftssparten, nicht nur beim *E-Commerce.* Es wird immer weniger Raum für eine Zusammenarbeit mit weniger transparenten und belastbaren Organisationen geben, vor allem diejenigen, die fahrlässig auftreten;

2. Unternehmensharmonisierung heißt die Überwindung der typischen Abteilungstrennungen.

Die Übung der Analyse und Identifizierung der aktuellen Daten und ihrer Flüsse in Unternehmen wird es ermöglichen, die Rolle eines jeden Beteiligten in den verschiedenen Prozessen besser zu identifi-

Novas oportunidades de negócio trazem consigo mudanças, muitas vezes associadas à incorporação de novas tecnologias (logo novos riscos de Cibersegurança), que não sendo devidamente acautelados, tornam-se alvo de ciberameaças como a *Ransomware* ou espionagem industrial (ex. por *Advanced Persistent Threats residentes*). Assim, a adopção de frameworks de boas práticas de IT empresarial e de segurança de informação são cada vez mais um valor acrescentado.

Mas afinal o que tem a Cibersegurança a ver com o RGPD?

Como comecei por referir no início do artigo, entre outros impactos. A rentabilização destas medidas na consultoria novos processos, educação/treino dos colaboradores e também em tecnologia (q.b.) levará a mudanças na cultura empresarial, à responsabilização de cada um dos colaboradores para a sua missão e à conquista de oportunidades, que como escreveu Sun Tzu na sua obra épica, *Art of War, "In the midst of chaos there Is also opportunity".*

zieren (RACI). Die Einhaltung der DSGVO wird zum Abriss dieser unsichtbaren Hindernisse führen und die Transparenz, den Wissensaustausch und die notwendigen Synergien fördern, um auf die immer größeren Wettbewerbs- und Effizienzherausforderungen zu reagieren, d.h. die Synergie zwischen Abteilungen fördern;

3. Verringerung und Ausmerzung maliziöser Datenflüsse im Unternehmen

Das Wissen und die Dokumentierung von firmeninternen Datenflüssen, die in den entsprechenden Geschäftsprozessen gelistet werden, legen verdächtige Datenaktivitäten in der Organisation offen, vor allem nach außen hin (z.B. DLPs). Die Verbesserung der Informationssicherheitssysteme in Firmen, die Reife der Mitarbeiter, die Kenntnis über die gängigen Prozesse, machen es einem (internen oder externen) Angreifer wesentlich schwerer, unentdeckt zu bleiben, wenn er (durch irgendeines der Attribute C.I.A + R) die Daten der Körperschaft (einschließlich Personendaten) gefährdet.

4. Risiko, Risikoanalyse und Risikoeindämmung

Die diversen Schritte in Richtung Konformität werden es ermöglichen, die Datenrealität in den Organisationen (Speicherort, Kontrollen, Flüsse) besser kennenzulernen, was wiederum deren effektive Verwaltung ermöglicht. Existieren die in unserem Unternehmen verarbeiteten diversen Personendatenflüsse (und/oder PII-Daten – identifizierbare Personendaten), die Datenkategorien, in die sie sich einfügen, sowie die technischen und organisatorischen Maßnahmen, denen sie zu ihrem Schutz unterliegen, dann haben wir die notwendigen Elemente zur Risikoidentifizierung. Wurde erst einmal der Kontext identifiziert, das Verarbeitungsrisiko analysiert und eingeschätzt, dann können wir es behandeln. Hierbei handelt es sich um eine fundamentale Anforderung für die Governance der *Stakeholder.*

Es liegt an uns, die Chancen zu nutzen. Und denken Sie dabei an das afrikanische Sprichwort: "Wenn Du gläubig bist, dann bete, aber bewege auch die Füße". \\ **Tradução: Thomas Kaiser**

Der Autor

Fachmann für unternehmerische Informationssicherheit, gelernter Elektronik- und Telekommunikationsingenieur, postgraduiert in Informationssicherheits-management mit europäischer Befähigung als Datenschutzbeauftragter (Data Protection Officer). Sich für die Herausforderungen der CyberSecurity und der Digitalen Privatsphäre in der modernen Gesellschaft begeisternd, ist er Berater für Datenschutz und Sicherheit bei der Fa. Closer Consulting. \\

Die Übung der Analyse und Identifizierung der aktuellen Daten und ihrer Flüsse in Unternehmen wird es ermöglichen, die Rolle eines jeden eteiligten in den verschiedenen Prozessen besser zu identifizieren (RACI).

O exercício de análise e identificação, dos dados actuais e dos seus fluxos nas organizações, permitir identificar o papel de cada interveniente nos diversos processos (RACI).

Assim, apenas para citar algumas:

1. *Compliance is the new sexy*

A conformidade regulamentar será naturalmente um factor de alavanca para novos negócios, parcerias e investimentos com organizações igualmente conformes, que só admitirão a colaboração interpares. A privacidade de dados é já critério diferenciador das atividades online em todos os verticais de negócio, não só no e-commerce. Haverá cada vez menos espaço para a colaboração com organizações menos transparentes e menos resilientes, sobretudo as que se mostrarem negligentes;

2. Harmonização organizacional, a destituição das típicas "quintas" departamentais

O exercício de análise e identificação, dos dados actuais e dos seus fluxos nas organizações, permitir identificar o papel de cada interveniente nos diversos processos (RACI). A conformidade com o RGPD contribuirá para a dissolução destas barreiras invisíveis e catalisando a transparência, partilha de conhecimento e sinergias necessárias para responder aos desafios crescentes da competitividade e eficiência, ie, promovendo sinergias entre departamentos;

3. Diminuição e extinção de fluxos de dados maliciosos dentro da organização

O conhecimento e a documentação dos fluxos internos de dados, mapeados nos respectivos processos de negócio, permitem alertar para atividades suspeitas de dados na organização e especialmente para fora de portas (ex. DLPs). A melhoria da segurança dos sistemas de informação das organizações, da maturidade dos colaboradores, do conhecimento dos processos habituais, faz com que se torne muito mais complicado um atacante (interno ou externo) não ser detetado a comprometer (qualquer um dos atributos C.I.A + R) os dados da entidade (incluindo pessoais).

4. Risco, análise de risco e mitigação do Risco

Os diversos passos do processo de conformidade permitem conhecer a realidade dos dados nas organizações (localização, controlos, fluxos) o que permite a sua gestão efectiva. Quando temos na nossa posse os diversos fluxos de dados pessoais que processamos na organização (e/ou dados PII – dados pessoais identificáveis), as categorias de dados em que se enquadram, as medidas técnicas e organizativas a que estão sujeitos para a sua salvaguarda, temos os elementos necessários para a identificação do Risco. Definido o contexto, analisado e avaliado o Risco do processamento, podemos tratá-lo. Trata-se de um requisito fundamental para o Governance dos *stakeholders.*

Está nas nossas mãos potenciar oportunidade. E lembre-se do provérbio africano: "Se é religioso reze. Mas mexa os pés". \\ *Neste texto não foram aplicadas as regras do acordo ortográfico.*

O Autor:

**"Profissional de Segurança de Informação empresarial, engenheiro de Electrónica e Telecomunicações de formação, pós-graduado em Gestão da Segurança da Informação com certificação europeia em Privacidade de Dados Pessoais (Data Protection Officer). Apaixonado pelos desafios da Cibersegurança e da Privacidade Digital na sociedade moderna, é consultor de Privacidade e Segurança na Closer Consulting." **