ARMIS TELLES

MICROSOFT DATA COMPLIANCE ASSESSMENT TOOL (DCAT)

What is the Microsoft Data Compliance Assessment Tool (DCAT)

A comprehensive engagement created to help our customers define a clear hands-on approach strategy for IT and legal compliance

Identify and understand your **data processing compliance** status and **associated risks**, through a holistic approach: legal, organizational and security

Provide custom **expert advice** on the measures that need to be implemented in order to **reduce the risks** of non-compliance with **data protection rules**

Get **guidance and recommendations** for risk and compliance mitigation

ARMIS TELLES

Free in-depth Data Compliance consultation

DCAT is a Microsoft data compliance-driven tool to help clients assess the degree of compliance in your company's data processing and minimize the risks associated with fines, litigation, reputation, offering you protection for the future.

Microsoft is offering you a free data compliance assessment to give clients insight into potential vulnerabilities in your legal and IT environment.

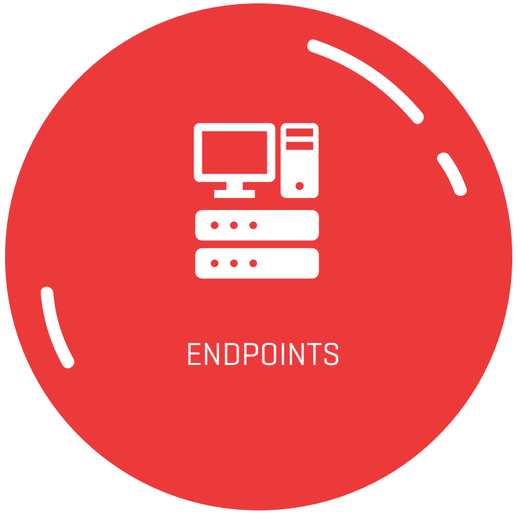
To perform the assessment, we will connect you with our teams of experts (legal and IT) to guide you through the assessment.

A report will be provided at the end to help you address and tackle identified red flags that may represent a liability risk to your company.

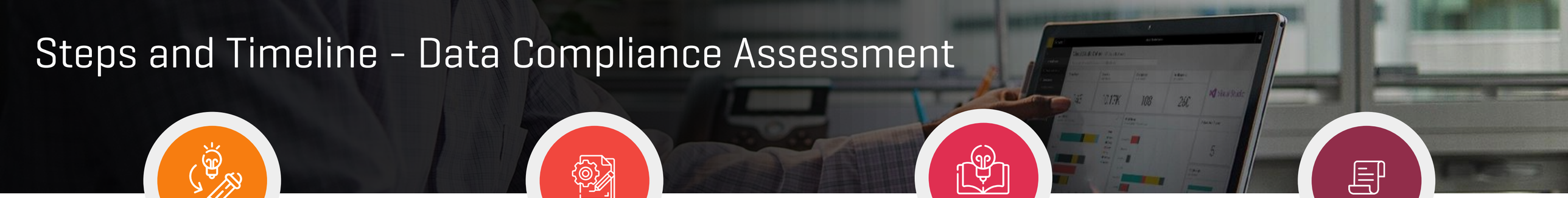
ARMIS TELLES

Free in-depth Data Compliance consultation

DCAT IN AN SET OF TOOLS PROVIDING AN EASY INTERFACE FROM WHICH YOU CAN COLLECT RELEVANT DATA FROM THE FOLLOWING SOURCES:



Steps and Timeline - Data Compliance Assessment



LEGAL AND IT MANAGER
CIO+CISO
COUNSEL+DPO+Sponsor

STEP 1

Let's get you started!

- Set-up a kick-off call with the Data Compliance team to:
  - Make introductions
  - Discuss the metodhology of the Questionnaire
  - Discuss goals of the assessment
- List business requirements based in existing functionalities
- High level understanding of risks and impacts moving forward
- Prepare your environment for the assessment and plan the next activities

1 Day

DATA MANAGERS

STEP 2

You answer to our Compliance Questionnaire

- The assessment begins with a questionnaire
- You will be asked to answer our question with information about your company and how it processes personal data.
- One of our Data Protection experts will be available to you to clarify any doubts you might have during this process

2 Days

Data Managers + Sponsor

STEP 3

We collect and analyse your data

- We analyse your answers and ask for relevant documentation
- Working sessions to understand the organization approach regarding legal, privacy, regulatory and security aspects Tools Execution and data discovery technical sessions.
- In some cases it might be required to do some on-site validations (legal documents, data discover and investigate risk scans).
- "Final Report" Elaboration

1 Weeks

LEGAL AND IT MANAGER
CIO+CISO
COUNSEL+DPO+Sponsor

STEP 4

Report Presentation

- Deliver presentation and discuss findings, conclusions and recommendations.
- Share "Final report" and presentation
- The content of the "Final Report" includes
  - Gap analysis
  - Recommendations
  - Road Map

2 Days

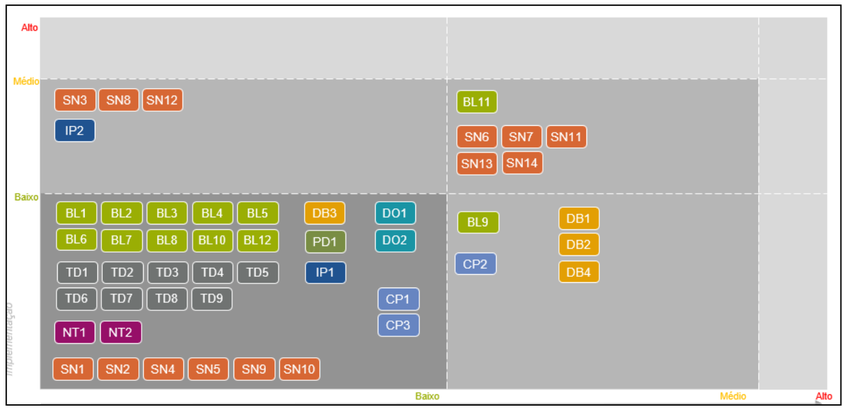
ARMIS TELLES

Non Compliance with the GDPR

Governo e Políticas | **Tratamentos de Dados** | Direitos dos Titulares | Proteção da Informação | Entidades Externas

Requisitos / Controlos	Descrição	A	Risco
B1. Interlocutor Designado para os Tratamentos de Dados Artigo 5.º do RGPD	Não se encontra formalmente definida a responsabilidade interna dos colaboradores (ou conjunto de colaboradores) da Sociedade pelos tratamentos de dados efetivamente realizados. A Sociedade deverá identificar um interlocutor para cada tratamento de dados e as suas responsabilidades no contexto da proteção dos dados pessoais.	●	Baixo
B2. Registo dos Tratamentos Artigo 30.º do RGPD	Foi realizada uma inventariação dos tratamentos de dados pessoais efetuados pela Sociedade. O processo de inventariação realizado não constitui, contudo, uma ferramenta de conformidade nos termos da legislação aplicável. Sugere-se a criação de um registo de atividades de tratamento, que deverá ser preenchido, completado e mantido atualizado para que a Sociedade cumpra as obrigações do RGPD e se encontre munida de uma ferramenta que auxilie os procedimentos de fiscalização a realizar, eventualmente, pela Autoridade de Controlo (CNPD).	○	Alto
B3. Consentimento (Geral) Artigos 6.º, 7.º e 9.º RGPD	Foram identificadas situações em que o consentimento não cumpre os requisitos impostos pela legislação aplicável, não sendo, inclusive, o fundamento de licitude adequado para o tratamento dos dados pessoais, p.ex.: (i) no recebimento de dados em processos de recrutamento; (ii) na divulgação de dados pessoais dos trabalhadores em redes sociais; (iii) na angariação de clientes; (iv) na recolha de dados de terceiros (agregado familiar) para efeitos de celebração de seguros de saúde; (v) no tratamento de dados de saúde, no caso de reclamações e incidentes; ou (vi) mesmo na realização das respetivas atividades de marketing direto ou inquéritos de opinião.	●	Alto
B4. Categorias especiais de dados pessoais Artigo 9.º RGPD	Identificou-se a recolha de dados de saúde (pelo distribuidor) no âmbito de reclamações, em caso de incidente ou se o produto se demonstrar não conforme com as normas de qualidade aplicáveis ao setor. A receção das informações e relação com os distribuidores deverá ser analisada e, se necessário, restringida ou alterada de modo a salvaguardar o tratamento de dados em conformidade com a legislação aplicável. Poderá ser necessário a criação de um ponto de contacto direto entre os cliente finais e a Sociedade, onde seja recolhido, por exemplo, o consentimento. A recolha e dados de saúde nos moldes expostos poderá ser potencialmente ilícita. Identificou-se a recolha de dados biométricos dos trabalhadores para o controlo de acessos. O processo de recolha deve ser analisado em conformidade com a legislação aplicável, incluindo no âmbito da Avaliação de Impacto para a Proteção de Dados Pessoais.	○	Alto
B5. Limitação dos dados pessoais	Identificaram-se situações em que os dados não são limitados ao estritamente necessário à finalidade prosseguida, p.ex., na gestão de clientes para fins comerciais são recolhidos os dados de aniversários das famílias dos respetivos clientes. As atividades de tratamento devem ser revistas de modo a respeitarem o princípio da minimização dos dados pessoais.	●	Médio

Avaliação (A): ● Conformidade Parcial ○ Em inconformidade



What will we deliver to your company?

- Maturity model and questionnaire
- Data protection findings and recommendations
- Technical data to detect potential vulnerabilities and to help prioritize next actions
- Actions to improve data compliance (urgent action items and quick wins)
- Overview of recommended legal measures, review recommendations to mitigate risks identified and improvements mapped to solutions

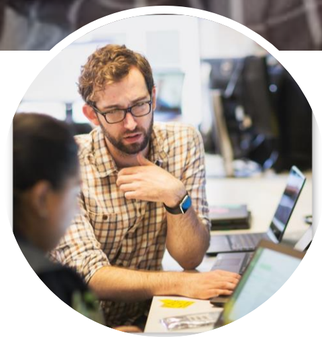
The Data Compliance assessment will help you...

ALIGN

- GDPR, ePrivacy and ISO 27001 requirements...
- IT/Risk Management and Data Protection shares fact-based risk and compliance conclusions and recommendations with Business Management
- Offers risk-based action plan for security and compliance improvements

OPTIMIZE

- Saves money if available Microsoft licenses are deployed
- Prevents deployment of point solutions



CONTROL

- Proves that you take data privacy and security seriously
- Shows that you work towards compliance

NUNO ANTUNES

(+351) 962 095 550
nuno.antunes@armisgroup.com

RUI COSTA

(+351) 962 095 582
rui.costa@armisgroup.com

ARMIS

(+351) 226 002 295
Rua do Freixo, nº 725-B,
4300-217 Porto
info@armisgroup.com