TREIO
TRaining on European Investigation Order

O Sistema de Intercâmbio Digital de Provas e-Evidence Digital Exchange System (eEDES)

Procuradoria Geral da República, 11 de Novembro de 2022
Júlio Barbosa e Silva

Este projeto foi financiado pelo Programa de Justiça da União Europeia (2014-2020) sob o Contrato de Subvenção nº 882068

Módulo 1, Sessão 1.1
‘Âmbito da DEI como instrumento’

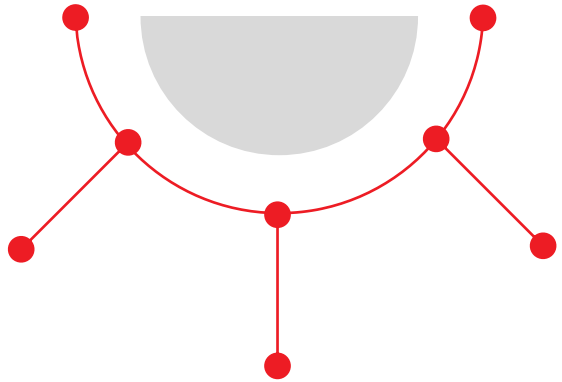
Visão geral do Módulo 1, Sessão 1.1

A sessão 'Âmbito da DEI como instrumento' do Módulo 1 cobre:

- Visão geral dos instrumentos jurídicos de cooperação
- O que é uma DEI?
- Âmbito de uma DEI
- Quando não usar uma DEI
- Quadro jurídico dentro do qual emitir e executar a DEI

INSTRUMENTOS JURÍDICOS DA EU PARA COOPERAÇÃO

Escolha do instrumento certo para atender às suas necessidades



Convenção Relativa ao Auxílio Judiciário Mútuo2000

Usar com Dinamarca e Irlanda

Usar para entrega de documentos

Regulamento (UE) 2018/1805

Para solicitar o congelamento e apreensão de bens no âmbito do processo em matéria penal

Diretiva 2014/41/UE

Usar na realização de qualquer medida investigatória

Para todos os EM, exceto Dinamarca e Irlanda

CONVENÇÃO 2000

É a base para a auxílio judiciário mútuo para assuntos que não se enquadram no âmbito da Diretiva DEI, por exemplo, envio de peças processuais, troca espontânea de informações, restituição de objetos às vítimas, etc.

IRLANDA E DINAMARCA

- A Irlanda e a Dinamarca optaram por não aderir à Diretiva DEI

- Os pedidos para obtenção de provas por parte da Irlanda e da Dinamarca são efetuados ao abrigo da Convenção 2000 e protocolo adicional sobre Auxílio Judiciário Mútuo em Matéria Penal

O QUE ACONTECE SE UMA DEI FOR ENVIADA PARA A IRLANDA E DINAMARCA POR ENGANO? (1)

- A Dinamarca trata uma DEI enviada por engano como uma Carta Rogatória e não exige um novo pedido de auxílio judiciário;

- Importante lembrar que a CR é executada com base na lei processual penal dinamarquesa e não com base no reconhecimento mútuo como no âmbito da DEI.

O QUE ACONTECE SE UMA DEI FOR ENVIADA PARA A IRLANDA E DINAMARCA POR ENGANO? (2)

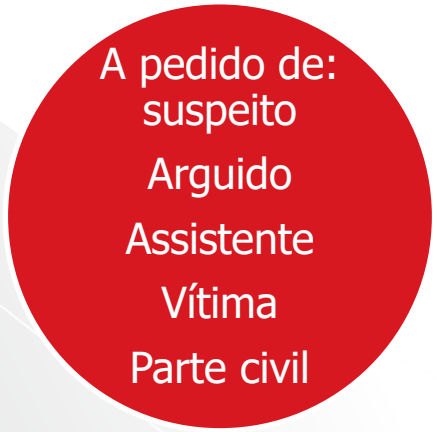
- A Irlanda não tem jurisdição legal para executar qualquer DEI, mas reconhecerá uma CR que vise a mesma prova e seja emitida com base na Convenção do Conselho da Europa de 1959 ou na Convenção 2000, ou ambas, e fará o possível para executá-la de acordo com a legislação nacional.
- De acordo com um relatório recente da Eurojust, "[o] facto de nas relações com a Irlanda e a Dinamarca o princípio do reconhecimento mútuo não se aplicar no contexto da recolha de provas não significa necessariamente que tais pedidos sejam inevitavelmente longos e incómodos. Por exemplo, num caso em que um Estado-Membro solicitou assistência à Irlanda, todas as medidas solicitadas foram executadas em menos de 3 dias."

REINO UNIDO

- Quanto ao Reino Unido
  - Até 31 de dezembro de 2020 – as DEI foram executadas (em conformidade com as disposições da Diretiva)
  - Desde 1 de janeiro de 2021 – Todos os pedidos para o Reino Unido são processados como MLA/AJM e seguem via Autoridade Central (PGR);
- Os pedidos de AJM entre os estados membros da UE e o Reino Unido são agora baseados na cooperação através:
  - da Convenção do Conselho da Europa de 1959 sobre Auxílio Judiciário Mútuo em Matéria Penal
  - dos seus dois protocolos adicionais, complementados pelas disposições acordadas no Título VIII do Acordo de Comércio e Cooperação UE-Reino Unido.

ATORES ENVOLVIDOS

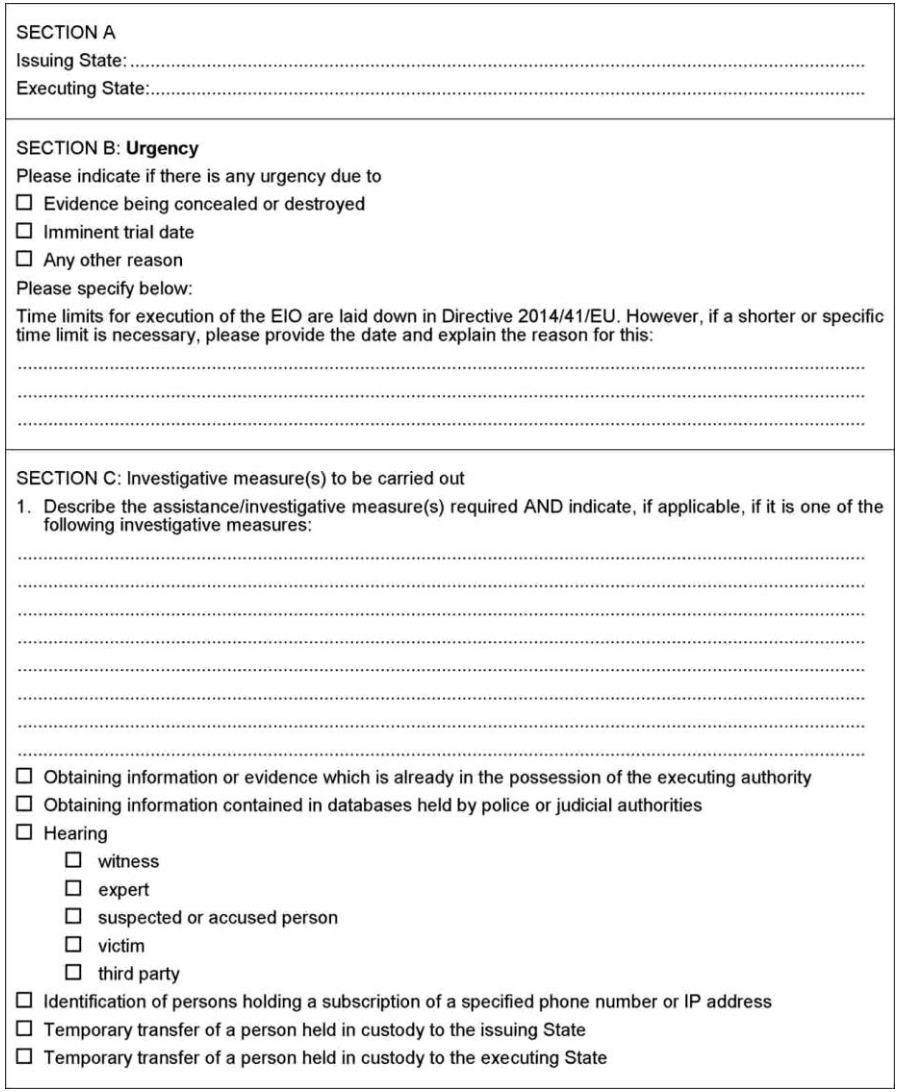
Ou, em alternativa, com base na lei interna



DEI

FORMULÁRIO DEI

- Previsto no Anexo da Diretiva
- A DEI contém particularmente:
  - dados relativos à autoridade de emissão e, se aplicável, à autoridade de validação;
  - o seu objeto e justificação;
  - as informações necessárias que estejam disponíveis acerca da pessoa ou pessoas em causa;
  - uma descrição da infração penal que é objeto da investigação ou do processo, e as disposições de direito penal do Estado de emissão aplicáveis;
  - uma descrição da medida ou medidas de investigação solicitadas e das provas a obter.



SECTION A

Issuing State: .....

Executing State: .....

SECTION B: **Urgency**

Please indicate if there is any urgency due to

☐ Evidence being concealed or destroyed

☐ Imminent trial date

☐ Any other reason

Please specify below:

Time limits for execution of the EIO are laid down in Directive 2014/41/EU. However, if a shorter or specific time limit is necessary, please provide the date and explain the reason for this:

.....

.....

.....

SECTION C: Investigative measure(s) to be carried out

1. Describe the assistance/investigative measure(s) required AND indicate, if applicable, if it is one of the following investigative measures:

.....

.....

.....

.....

.....

.....

.....

.....

☐ Obtaining information or evidence which is already in the possession of the executing authority

☐ Obtaining information contained in databases held by police or judicial authorities

☐ Hearing

- ☐ witness
- ☐ expert
- ☐ suspected or accused person
- ☐ victim
- ☐ third party

☐ Identification of persons holding a subscription of a specified phone number or IP address

☐ Temporary transfer of a person held in custody to the issuing State

☐ Temporary transfer of a person held in custody to the executing State

Seção A-C do Anexo A, Diretiva EIO

LÍNGUA DA DEI

- O artigo 5.º, n.º 2, da Diretiva DEI exige que "Cada Estado-Membro indique, de entre as línguas oficiais das instituições da União e além da língua oficial ou línguas oficiais do Estado-Membro em causa, a língua ou línguas que podem ser utilizadas para preencher ou traduzir a DEI quando o Estado-Membro em causa for o Estado de execução".
- Lista de idiomas no documento da RJE intitulado "*Autoridades competentes, línguas aceites, questões urgentes e âmbito de aplicação da Diretiva.*"

Desafios	Efeito
Qualidade das traduções não muito boa	A DEI não pode ser executada (pois não foi entendida)
Traduções em falta	DEI considerada incompleta e não pode ser executada

ÂMBITO DE UMA DEI

- "a DEI abrange **qualquer medida de investigação**" (Artigo 3.º da Diretiva DEI)

- Os seguintes critérios podem ser úteis para avaliar se a Diretiva DEI deve ser aplicada:
  - a decisão diz respeito a uma medida de investigação para recolher ou utilizar provas
  - a medida foi emitida ou validada por uma autoridade judiciária
  - a medida diz respeito aos Estados-Membros vinculados pela Diretiva DEI

NÃO INCLUÍDO NO ÂMBITO DA DEI (1)

- Excluído da DEI
  - A criação de uma equipa de investigação conjunta e a recolha de provas no seio dessa equipa (artigo 3.º da Diretiva DEI)
  - Vigilância transfronteiriça (conforme referido na Convenção de Aplicação do Acordo de Schengen) (Considerando 9 da Diretiva DEI)
  - Citação e envio de atos processuais, a menos que a entrega de um documento seja instrumental para a medida investigativa objeto da DEI (Convenção AJM 2000)
  - Troca espontânea de informações (Artigo 7.º da Convenção AJM 2000)
  - Transferência de processos (Artigo 21 da Convenção de 1959 do Conselho da Europa sobre Auxílio Judiciário Mútua de 1959 e Convenção do Conselho da Europa de 1972 sobre Transferência de Processos em Processos Criminais)

NÃO INCLUÍDO NO ÂMBITO DA DEI (2)

- Excluído da DEI
  - Congelamento de bens para efeitos de apreensão posterior (Regulamento 2018/1805 sobre o reconhecimento mútuo das decisões de apreensão e perda)
  - Restituição: devolução de um objeto à vítima (Artigo 8.º da Convenção AJM 2000)
  - Recolha de extratos do registo criminal (através do Sistema Europeu de Informação sobre Registos Criminais – ECRIS , na sequência da Decisão-Quadro 2008/675/JAI do Conselho, de 24 de julho de 2008, relativa à tomada em consideração das condenações nos Estados-Membros da União Europeia no decurso de novo processo penal)
  - Cooperação entre polícias
  - Cooperação alfandegária

Lei Aplicável para Execução da DEI

- A **execução** é regida pela **lei do Estado-Membro de execução.**

- MAS a autoridade de execução deve cumprir as formalidades e procedimentos expressamente indicados pela autoridade de emissão, 'desde que não sejam contrários aos princípios fundamentais do direito do Estado de execução'. (Artigo 9.º, n.º 2, Diretiva DEI)

Momento de Emissão de uma DEI

- Todas as fases do processo penal, incluindo a fase de julgamento (Considerando 25 da Diretiva DEI) e fase de execução de sentença, desde que vise recolha de provas;

- Se trazido por uma autoridade administrativa ou judicial relativa a uma infração penal, ou infrações que possam levar a acusação criminal

DIREITOS FUNDAMENTAIS E A DEI

- A Diretiva DEI não afeta a natureza ou as obrigações dos próprios direitos fundamentais; "não terá o efeito de modificar a obrigação de respeitar os direitos fundamentais e os princípios jurídicos consagrados no artigo 6.º do TUE". (Artigo 1.º, n.º 4, da Diretiva DEI)
- As incompatibilidades com a Carta dos Direitos Fundamentais ou o artigo 6.º do TUE são um possível motivo para o não reconhecimento ou não execução de uma DEI (artigo 11.º, n.º 1, alínea f), da Diretiva DEI)
- Direitos fundamentais relevantes:
  - Privacidade (Artigo 7.º CDF)
  - Proteção de dados (Artigo 8.º CDF)
  - Igualdade perante a lei (Artigo 20.º CDF)
  - Recurso efetivo e julgamento justo (Artigo 47.º CDF)
  - Presunção de inocência (Artigo 48.º CDF)
  - Direito de não ser julgado ou punido duas vezes (artigo 50.º CDF)
  - Disposições relevantes da Diretiva DEI: considerando 12, 17, 18, 39

Proteção de Dados e a DEI

- Considerando 40 da Diretiva DEI: A proteção das pessoas singulares no que toca ao tratamento de dados é um direito fundamental. Em conformidade com o artigo 8.º, n.º 1, da Carta e o artigo 16.º, n.º 1, do TFUE**, todas as pessoas têm direito à proteção dos dados de caráter pessoal** que lhes digam respeito.
- A emissão ou execução de um pedido de uma DEI frequentemente requer o tratamento de dados pessoais
- A **legislação secundária** (RGPD e Diretiva 2016/680) defende o direito fundamental ao permear todas as circunstâncias do tratamento de dados pessoais
- Estes dois atos legislativos aplicam-se isoladamente um do outro (âmbito distinto e **aplicação mutuamente exclusiva**)
- Normalmente, a **DAL aplica-se** quando uma DEI é emitida ou executada

ENQUADRAMENTO PD APLICÁVEL (DIRETIVA 2016/680, RGPD)

- Artigo 20 da Diretiva DEI

  *Ao aplicar a presente diretiva, os Estados-Membros **devem assegurar que os dados pessoais sejam protegidos** e só possam ser tratados nos termos da Decisão-Quadro 2008/977/JAI do Conselho (1) e de acordo com os princípios consagrados na Convenção do Conselho da Europa […]*

- Dado que a Diretiva 2016/680 revogou a 2008/977/JAI e fornece a base jurídica da UE para o tratamento e intercâmbio de dados pessoais no contexto da **cooperação judiciária em matéria penal** e da cooperação policial, a Diretiva 2022/228, de 6 de Fevereiro de 2022 alterou a Diretiva DEI no que diz respeito à sua harmonização com as regras da União em matéria de proteção de dados pessoais, suprimindo o artigo 20.º.

ENQUADRAMENTO PD APLICÁVEL (DIRETIVA 2016/680, RGPD)

- A Diretiva 2016/680 estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais

  *pelas **autoridades competentes** para **efeitos** de **prevenção, investigação, deteção ou repressão de infrações penais** ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.*

- A Diretiva 2016/680 prevê um nível mínimo de harmonização
- A Diretiva 2016/680 e as disposições legais nacionais de transposição devem ser observadas

- Nos casos em que a Diretiva 2016/680 não se aplica, por exemplo, no que diz respeito ao tratamento de dados pessoais em relação aos processos referidos no artigo 4.º, alíneas b), c) e d) (da Diretiva DEI), aplica-se o Regulamento 2016/679 (o RGPD).

RESPONSABILIZAÇÃO

- Dependendo das circunstâncias específicas, tanto as partes emitentes como as executoras das DEI podem ser **responsáveis pelo tratamento ou subcontratantes**
- A equiparação das funções de proteção de dados depende das **funções e responsabilidades** dos atores da DEI
- O responsável pelo tratamento é a entidade que determina as **finalidades e os meios de tratamento** de dados pessoais
- O responsável pelo tratamento deve realizar a seguinte avaliação para cumprir a Diretiva 2016/680

  > *tendo em conta a **natureza, o âmbito, o contexto** e as **finalidades do tratamento** dos dados, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, aplique as **medidas técnicas e organizativas adequadas** para assegurar e poder comprovar que o tratamento é realizado em conformidade com a presente diretiva. Estas medidas são avaliadas e atualizadas, se necessário*

- O **ónus** é, portanto, **do responsável pelo tratamento** para interpretar e implementar corretamente a lei de acordo com a DAL em todo o tratamento de dados

ENQUADRAMENTO PD APLICÁVEL (DIRETIVA 2016/680, RGPD)

- Artigo 20 da Diretiva DEI

  *Ao aplicar a presente diretiva, os Estados-Membros **devem assegurar que os dados pessoais sejam protegidos** e só possam ser tratados nos termos da Decisão-Quadro 2008/977/JAI do Conselho (1) e de acordo com os princípios consagrados na Convenção do Conselho da Europa […]*

- Dado que a Diretiva 2016/680 revogou a 2008/977/JAI e fornece a base jurídica da UE para o tratamento e intercâmbio de dados pessoais no contexto da **cooperação judiciária em matéria penal** e da cooperação policial, a Diretiva 2022/228 suprimiu o artigo 20.º (em fevereiro de 2022).

Responsabilização, Princípios, Direitos do Titular dos Dados e Responsabilidades Adicionais

- A Diretiva 2016/680 exige que as entidades que tratam dados pessoais assumam o papel de **responsável pelo tratamento** ou **subcontratante**
- Os responsáveis pelo tratamento são os principais tomadores de decisão - exercem controlo geral sobre as **finalidades e meios** da atividade de tratamento
- Responsabilidade do responsável pelo tratamento: aderir aos requisitos da Diretiva 2016/680
  - **princípios** do tratamento
  - manutenção dos **direitos dos titulares dos dados**
  - **outras obrigações**

} **demonstrar conformidade**

Princípios da Proteção de Dados (1/3)

- O artigo 4.º da Diretiva 2016/680 estabelece os **princípios fundamentais da proteção de dados** – de acordo com as disposições, cabe aos Estados-Membros a responsabilidade de garantir a conformidade
- Licitude e lealdade (exceto transparência e consentimento), limitação de finalidades, minimização de dados, exatidão, limitação da conservação, segurança de dados, responsabilidade
- Dadas as finalidades de tratamento, alguns desvios ao RGPD podem ser observados, como a omissão de 'transparência' ou consentimento como base legal
- Em termos de **licitude** do tratamento, o tratamento deve, nos termos do artigo 8.º da Diretiva 2016/680, '*ser **necessário** para o exercício de uma **atribuição pela autoridade competente** para os efeitos previstos no artigo 1.º, n.º 1, e tiver por **base** o **direito** da União ou de um Estado-Membro*.

PRINCÍPIOS DA PROTEÇÃO DE DADOS (2/3)

- O princípio da '**lealdade**' vai além da transparência e tem conexões éticas (tratamento objetivo e imparcial dos titulares dos dados)
- A '**limitação das finalidades**' exige que os dados pessoais sejam recolhidos para 'finalidades determinadas, explícitas e legítimas'. A Diretiva 2016/680 apresenta uma ligeira variação de termos em relação ao RGPD, pois afirma que os dados pessoais devem ser adequados, relevantes e 'não excessivos' (em comparação com 'limitados ao necessário') em relação às finalidades para os quais são tratados.
- O princípio da '**exatidão**' exige que os dados pessoais sejam *'exatos e atualizados sempre que necessário; devem ser tomadas todas as medidas razoáveis para que os dados inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora'*.

Princípios da Proteção de Dados (3/3)

- A '**limitação da conservação**', em princípio afirma que os dados pessoais devem ser mantidos de uma forma que permita a identificação dos titulares dos dados por não mais do que o necessário para os fins para os quais são tratados;
- O princípio da '**integridade e confidencialidade**', segundo o qual os dados pessoais devem ser *tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas*. O artigo 19.º da Diretiva DEI, intitulado 'Confidencialidade', reflete o objetivo das disposições de segurança contidas na Diretiva 2016/680 e reitera as responsabilidades de confidencialidade
- Os princípios contribuem para a proteção dos direitos do titular dos dados, fornecendo **responsabilidade** por parte do responsável pelo tratamento

Direitos dos Titulares dos Dados

- O **titular dos dados** é uma 'pessoa singular identificada ou identificável'
  - A Diretiva DEI diz que '*o acesso a esses dados é restrito,* ***sem prejuízo dos direitos do titular dos dados***'
  - O Capítulo III da Diretiva 2016/680 estabelece os direitos dos titulares dos dados, incluindo o direito de acesso, o direito de retificação ou atualização dos seus dados, o direito de solicitar o apagamento, ou o direito de restringir ou opor-se ao tratamento em causa, etc.
  - A Diretiva 2016/680 permite que os Estados-Membros prevejam certas **limitações** nas suas **transposições nacionais** para estes direitos
- Ao longo dos procedimentos da DEI, os responsáveis pelo tratamento de dados e subcontratantes devem observar e respeitar os direitos do titular dos dados dentro da limitação prevista pelas transposições nacionais da Diretiva 2016/680

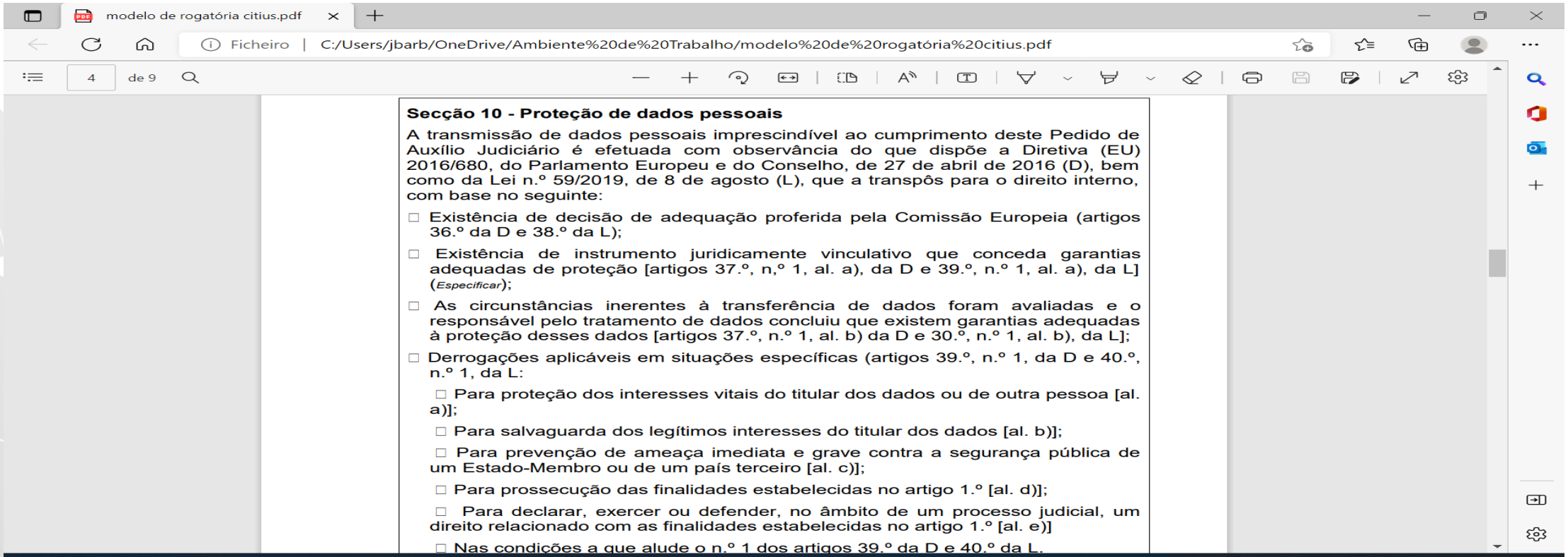
NECESSIDADE E PROPORCIONALIDADE

- O considerando 42 da Diretiva DEI afirma que '*dados pessoais obtidos ao abrigo da presente diretiva* ***só deverão ser tratados quando necessário, e deverão ser proporcionados*** *em relação aos fins compatíveis com a prevenção, a investigação, a deteção e do crime e o exercício da ação penal, ou com a aplicação de sanções penais e o exercício do direito à defesa*'
- Além disso, o artigo 6.º, n.º 1, alínea a), da Diretiva DEI estabelece que uma DEI só deve ser emitida quando a emissão da DEI for '*necessária e proporcionada para efeitos dos processos a que se refere o artigo 4.º, tendo em conta os direitos do suspeito ou do arguido*'
- A **necessidade e a proporcionalidade** da finalidade do processo estão diretamente relacionadas com a necessidade e a proporcionalidade subjacentes ao considerando 42 da Diretiva DEI e à **recolha e tratamento de dados pessoais**
- As considerações devem ser feitas de acordo com a finalidade, assunto, valor e meios de transferência de dados ao executar uma DEI e recolher e transferir evidências eletrónicas.

PROTEÇÃO DE DADOS – UMA "FEBRE" DA UE??

- Relevância da proteção de dados e implicação na Cooperação Internacional em matéria penal fora da UE?

- O modelo de Carta rogatória do CITIUS: o que se pretende ao certo?



PROTEÇÃO DE DADOS – UMA "FEBRE" DA UE??

Objetivos das informações apostas no formulário CR do Citius:

- Consciencializar da relevância das questões de proteção de dados e condicionamento da cooperação e/ou das provas obtidas; proteção de pessoas; perseguições políticas; sistemas sem garantias de uso apenas judiciário da informação;

(cerca de um terço do Regulamento da Procuradoria Europeia prende-se com questões de PD)

- A importância prende-se com Estados terceiros à UE, na medida em que neste espaço a circulação de dados é livre e existe legislação já transposta pelos EM (Diretiva 2016/680, de 27-04-2016, transposta em Portugal pela Lei 59/2019, de 8 de Agosto).
- As situações cairão numa destas hipóteses:

a) Existe decisão de adequação por parte da Comissão Europeia;
b) Existe avaliação positiva de um Estado de execução com standard de proteção de dados aproximado ao nosso;
c) Existe uma qualquer situação no âmbito do artigo 39º da Diretiva.

PROTEÇÃO DE DADOS – UMA "FEBRE" DA UE??

Quem faz essa avaliação de adequação em concreto para o futuro, se necessário?

- No futuro a PGR emite instruções/recomendações sobre procedimentos a levar a cabo pelo titular dos autos?

- Causa de recusa de emissão de CR?
- Como proceder se se pretende enviar uma CR para um Estado terceiro?

Ou se faz uma avaliação prévia sobre adequação ou numa das situações do artigo 39º.

(na Eurojust, por exemplo, antes de abrir caso com Estado terceiro, é pedido ao Colégio uma avaliação prévia sobre a adequação da legislação desse Estado relativo à proteção de dados)

Recomendações superiores podem autorizar o não envio de CR....

Como fica a cooperação nestes casos de avaliação negativa ou falta de avaliação? Impossibilidade de cooperação?! Com todos os países sem standard europeu ou aproximado?!

(importância para a prova e sua validação bem como para a investigação)

Eventual papel da PGR para o futuro no âmbito destas considerações?