

Julho de 2020

Magda Cocco | [mpc@vda.pt](mailto:mpc@vda.pt)  
Inês Antas de Barros | [iab@vda.pt](mailto:iab@vda.pt)  
Maria de Lurdes Gonçalves | [mlg@vda.pt](mailto:mlg@vda.pt)

## COMUNICAÇÕES, PROTEÇÃO DE DADOS & TECNOLOGIA

### TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA INVALIDA EU-US PRIVACY SHIELD (CASO SCHREMS II)

No dia 16 de julho de 2020, o Tribunal de Justiça da União Europeia (**TJUE**) proferiu um acórdão marcante no Caso Schrems II (processo C-362/14), tendo, como já era expectável, decidido pela invalidade do EU-US Privacy Shield, um dos mecanismos utilizados para a transferência de dados pessoais para os EUA. No seu acórdão, o TJEU teceu ainda algumas considerações relativamente à utilização do mecanismo assente nas Cláusulas Contratuais Tipo (**CCT**).

Na sequência desta decisão que produz efeitos imediatos, as organizações terão, necessariamente, de reavaliar os mecanismos utilizados para as transferências internacionais de dados pessoais e levar a cabo um conjunto de ações, por forma a assegurar o cumprimento dos requisitos do Regulamento Geral sobre a Proteção de Dados (**RGPD**).

#### ANTECEDENTES DO CASO SCHREMS

O caso Schrems remonta a 2015, quando Max Schrems contestou, junto da autoridade de controlo irlandesa, a validade do acordo de Safe Harbor - um dos mecanismos então utilizados para transferências internacionais de dados para os EUA.

A queixa de Schrems fundava-se na alegada falta de garantias do mecanismo do Safe Harbor relativamente à utilização de sistemas de vigilância estatais, nos termos da legislação norte-americana. Na sequência dessa queixa, o TJUE viria a invalidar o Safe Harbor, naquele que ficou conhecido como o acórdão Schrems I.

Em sua substituição, foi criado outro mecanismo – o Privacy Shield – que, à semelhança do Safe Harbor, constitui um esquema de auto-certificação, ao qual as empresas sedeadas nos EUA aderem, atestando a adequação das medidas de segurança, por si implementadas, para a proteção dos dados pessoais e direitos dos titulares.

Em 2018, retomou-se a discussão sobre a legalidade dos dois mecanismos mais utilizados para transferências de dados, nomeadamente o Privacy Shield e as CCT, naquele que foi denominado como caso Schrems II.

## **TRANSFERÊNCIAS INTERNACIONAIS & RGPD**

O RGPD prevê que as transferências de dados pessoais para fora do Espaço Económico Europeu só possam ser realizadas quando o país terceiro apresente um nível adequado de proteção dos dados pessoais, equivalente àquele que é conferido pela legislação europeia.

Caso não existam Decisões de Adequação emitidas pela Comissão Europeia para determinados países ou territórios (como sucede, por exemplo, para a Argentina, Canadá ou Suíça), as organizações, independentemente de serem responsáveis pelo tratamento ou subcontratantes, só podem transferir dados pessoais para um país terceiro se apresentarem garantias adequadas.

De entre as garantias previstas pelo RGPD, destacam-se mecanismos como as CCT ou as regras vinculativas aplicáveis às empresas (*Binding Corporate Rules*), a par do Privacy Shield (este último, apenas para transferências para os EUA). O RGPD prevê ainda outras circunstâncias que podem justificar a transferência internacional de dados sem recurso a estes mecanismos legais.

Uma vez que os EUA não foram objeto de uma Decisão de Adequação, as organizações que transferem dados para este país tipicamente recorriam, até à data, ao Privacy Shield ou à celebração das CCT com as entidades destinatárias dos dados.

## **CASO SCHREMS II: A DECISÃO DO TJUE**

### **1. UE-EUA Privacy Shield**

À semelhança do sucedido com o Safe Harbor, o TJUE invalidou o mecanismo do Privacy Shield por, em termos gerais, considerar que a legislação norte-americana não assegura os requisitos essencialmente equivalentes aos exigidos pela legislação europeia.

De facto, quando estejam em causa medidas que versem sobre segurança nacional e sobre o acesso a dados pessoais por autoridades públicas, o TJUE considera que, tal como previsto na Carta Europeia de Direitos Fundamentais, deve ser observado um conjunto de salvaguardas mínimas. Desde logo, (i) deve existir uma base legal, (ii) devem ser estabelecidos limites ao acesso aos dados e (iii) devem ser implementados procedimentos específicos que regulem tal acesso. O TJUE considerou que tais salvaguardas não estão acauteladas através da utilização do mecanismo do Privacy Shield.

Entre outros aspetos, o TJUE apontou ainda para a falta de tutela judicial efetiva dos direitos dos titulares – ou seja, a impossibilidade de recorrer a um tribunal para fazer valer direitos – em caso de utilização do Privacy Shield.

### **2. CCT**

As CCT são cláusulas contratuais aplicáveis às transferências de dados pessoais, aprovadas pela Comissão Europeia em 2010, e que podem ser celebradas entre organizações estabelecidas na UE e organizações destinatárias de dados estabelecidas fora do território da UE.

No acórdão proferido, o TJUE não invalidou a utilização das CCT, mas teceu algumas considerações que terão um impacto prático nas operações de transferências de dados.

O TJUE salientou que as organizações têm de confirmar, previamente à utilização das CCT, o nível de proteção efetivo assegurado pelas jurisdições para onde os dados são transferidos e, bem assim, se este nível de proteção é similar ao conferido na União Europeia.

Deste modo, o TJUE estabelece maiores exigências para os responsáveis pelo tratamento, em linha com o princípio da responsabilidade previsto no RGPD. O TJUE aconselha ainda as organizações a implementarem medidas de salvaguarda adicionais, embora não densifique que tipo de medidas.

No seguimento deste acórdão, será expectável que, tal como já estava previsto na Comunicação da Comissão Europeia de avaliação dos dois anos de aplicação do RGPD, as CCT venham a ser revistas por forma a acomodar estas considerações do TJUE.

## **PRÓXIMOS PASSOS PARA AS ORGANIZAÇÕES**

Devido à produção imediata de efeitos da decisão, todas as organizações que recorram ao mecanismo do Privacy Shield deverão identificar e implementar outro mecanismo para as transferências de dados para os EUA, sob pena de incumprimento do RGPD.

Assim, as organizações deverão:

- Fazer um levantamento das categorias e tipos de dados pessoais que estão a ser transferidos para fora do Espaço Económico Europeu, bem como a base legal utilizada;
- Identificar se transferem dados para organizações aderentes ao Privacy Shield;
- Identificar se transferem dados para organizações com base em CCT, avaliando a viabilidade de utilização das mesmas;
- Avaliar cuidadosamente o mecanismo de transferência de dados mais adequado ao caso concreto, de entre as opções do RGPD; e
- Fundamentar e documentar todas as opções.

Dois anos após a implementação do RGPD e face à comunicação da Comissão Europeia sobre o facto das transferências internacionais serem um ponto a melhorar, espera-se que, nos próximos meses, existam desenvolvimentos no panorama das transferências de dados pessoais para fora do espaço Económico Europeu.

Recomenda-se, assim, o acompanhamento da posição das autoridades de controlo que, na sequência da tomada de decisão do Comité Europeu para a Proteção de Dados, poderão vir a emitir orientações importantes.