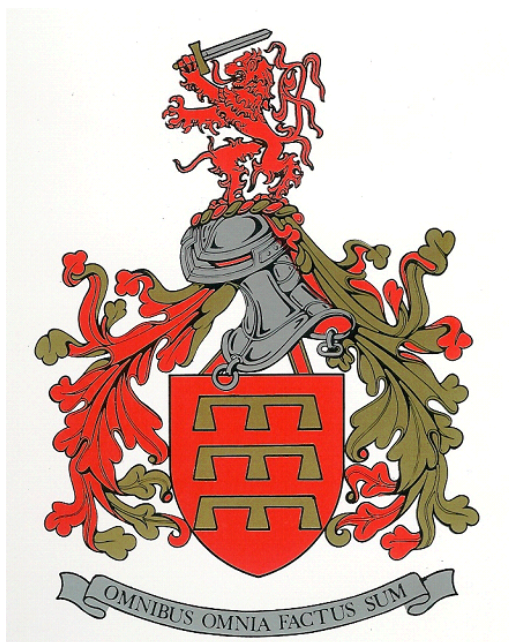


# MINISTÉRIO DA DEFESA NACIONAL

## EXÉRCITO PORTUGUÊS

### INSPEÇÃO-GERAL DO EXÉRCITO



#### Listas de Verificação

#### Auditorias de Proteção de Dados

**A - ORGANIZAÇÃO**P:  1**A1 - Pessoal-chave e outros**P:  1**A1.a - Responsável pelo Tratamento (RT) no Exército**P:  1

1 - O pessoal da U/E/O identifica corretamente a entidade máxima que determina as finalidades e os meios de tratamento de dados pessoais no Exército?

Av: P:  2**A1.b - Responsável pela Proteção de Dados (RPD) da U/E/O**P:  1

1 - Existe, foi nomeado em O.S. da U/E/O e a sua designação/substituição foi prontamente comunicada ao Encarregado de Proteção de Dados (EPD) do Exército?

Av: P:  3

2 - Enquanto Ponto de Contato (POC) da sua U/E/O para todos os assuntos respeitantes à Proteção de Dados pessoais, a sua identificação e contatos foram/estão amplamente divulgados a nível interno (p. ex. na página partilhada da U/E/O na intranet)?

Av: P:  2

3 - Encontra-se credenciado como superiormente determinado e as suas credenciações de segurança estão válidas?

Av: P:  2

4 - Está habilitado com a formação necessária ao desempenho da função?

Av: P:  3

5 - Conhece as responsabilidades e atribuições inerentes e detém experiência na função?

Av: P:  2

6 - Assiste e mantém o Cmdt/Dir/Ch prontamente informado sobre os assuntos de Proteção de Dados na sua U/E/O, propondo-lhe as m/a que se afigurem mais consentâneas para eventuais questões que surjam nesse domínio?

Av: P:  2

7 - Mantém ligação com o EPD do Exército para os aspetos inerentes à Proteção de Dados e ao RGPD, submetendo-lhe as questões que suscitem dúvidas ou ultrapassem a sua capacidade?

Av: P:  2

8 - Mantém-se em estreita ligação com o Oficial/Encarregado de Segurança (OfSeg/EncSeg) da U/E/O, para as questões de Segurança Militar com implicações na Proteção de Dados pessoais?

Av: P:  1

9 - Mantém-se em estreita ligação com o Administrador de Redes Locais (ARL) da U/E/O, para efeitos de Segurança das Comunicações e Sistemas de Informação com implicações na Proteção de Dados Pessoais?

Av: P:  1

10 - Tem promovido junto do Cmd/Dir/Ch, a realização periódica de palestras/ações de sensibilização/esclarecimentos do pessoal da U/E/O em matéria de Proteção de Dados pessoais?

Av: P:  1**A1.c - Oficial/Encarregado de Segurança (OfSeg/EncSeg) da U/E/O**P:  1

1 - Está designado e em funções?

Av: P:  1

2 - Mantém estreita ligação com o RPD da U/E/O, para as questões de Proteção de Dados com repercussões na Segurança Militar?

Av: P:  2**A1.d - Administrador de Redes Locais (ARL) da U/E/O**P:  1

1 - Está designado e em funções?

Av: P:  1

2 - Mantém ligação com o RPD da U/E/O, para as questões de Proteção de Dados com repercussões na Segurança das CSI?

Av: P:  2**A1.e - Consultor/Assessor Jurídico**P:  1

1 - A U/E/O dispõe organicamente de, ou pode ser apoiada por um consultor/assessor jurídico, desejavelmente, habilitado com formação especializada, no âmbito do RGPD e da Proteção de Dados?

Av: P:  1**A1.f - Comissão de Análise da Documentação (CAD)**P:  1

1 - A U/E/O dispõe de uma Comissão de Análise da Documentação nomeada e em exercício de funções?

Av: P:  1

**A1.g - Especialista de Documentação e Arquivo**P: 

1 - A U/E/O dispõe organicamente de, ou pode ser apoiada por pessoal habilitado na área de Biblioteca, Documentação e Arquivo ou de Gestão da Informação Arquivística?

Av:  P: **A2 - Segurança física +**P: **A2.a - Mentalidade e cultura de segurança e Proteção de Dados**P: 

1 - Existe noção generalizada no seio do Cmd/Dir/Ch e restante pessoal da U/E/O, de que os dados pessoais carecem de salvaguarda face à recolha, registo acesso, manuseamento e difusão indevidos, devendo ser unicamente objeto de tratamento, atentos o cumprimento da missão do Exército e as finalidades últimas da segurança e defesa do Estado?

Av:  P: 

2 - O pessoal da U/E/O está ciente dos cuidados a ter com passwords de segurança de bases de dados, estações de trabalho, redes e sistemas de informação, bem como com o manuseamento de documentação classificada, digital e impressa, em especial, que possam conter ou permitam aceder a dados pessoais?

Av:  P: **A2.b - Segurança do pessoa**P: 

1 - Para o acesso às Áreas de Segurança (Classes 1 e 2), Áreas Administrativas e Áreas Restritas da U/E/O, o pessoal é credenciado em função da "necessidade de conhecer", sendo a sua validade verificada/continuamente monitorizada?

Av:  P: 

2 - Existem listagens de acesso de entidades expressamente autorizadas a aceder a cada uma das áreas de segurança da U/E/O, afixadas junto às respetivas entradas e as mesmas estão atualizadas?

Av:  P: 

3 - Estão definidos e são efetivamente aplicados os procedimentos de registo, identificação, controlo de acessos e acompanhamento de trabalhadores externos, fornecedores de bens e serviços, indivíduos alheios e visitantes à U/E/O e respetivas áreas de segurança, administrativas e restritas?

Av:  P: **A2.c - Segurança das instalações**P: 

1 - Os dispositivos e sistemas de segurança existentes (i.e. vedação periférica, barreiras, iluminação, detetores de intrusão, videovigilância, controlo de acessos, alarmística, etc.) e as medidas complementares adotadas (i.e. guardas, rondas) garantem eficazmente a segurança face ao acesso indevido a dependências, infraestruturas e áreas onde possam existir repositórios de dados pessoais?

Av:  P: **A2.d - Segurança da informação e documental**P: 

1 - É feita a inventariação dos dados pessoais sob controlo da U/E/O, com a preocupação de a manter permanentemente atualizada?

Av:  P: 

2 - Estão definidas políticas e procedimentos de revisão dos dados pessoais armazenados, com vista à destruição dos que já não são necessários?

Av:  P: 

3 - O Cmdt/Dir/Ch da U/E/O tem diligenciado no sentido da proibição de criação, proliferação e utilização de quaisquer outras listagens, ficheiros, arquivos físicos e digitais e bases de dados pessoais, além dos que foram/estão superiormente autorizados?

Av:  P: 

4 - O dados pessoais estão encriptados nos servidores, de forma a que só possam a eles aceder as pessoas que necessitem da informação para o cumprimento de alguma finalidade e tenham permissão para o efeito?

Av:  P: 

5 - Existem no interior das áreas de segurança, cofres e armários apropriados (fechados com chave, fechadura de segredo ou tranca com cadeado), à prova de fogo, a fim de guardar os dados pessoais mais críticos e as cópias de segurança (backups)?

Av:  P: 

6 - Existem e são cumpridos pela U/E/O normativos e disposições de segurança superiormente aprovados e em vigor, relativos a chaveiros, controlo de chaves e combinações de segredo?

Av:  P: 

7 - A reprodução de documentos processa-se em fotocopiadoras fisicamente protegidas e manuseadas apenas por pessoal autorizado (p.ex. detentor de código de acesso ou outro)?

Av:  P: 

8 - Existem trituradoras para destruição de suportes físicos de informação (papel, CD/DVD, etc.) com diferentes capacidades, em função da área (de segurança, administrativa ou restrita) onde se localizam?

Av:  P:

9 - A destruição de suportes físicos de informação classificada contendo dados pessoais desnecessários é devidamente registada, acompanhada pelo RPD da U/E/O e elaborado o correspondente certificado de destruição?

Av:  P:  1

### A3 - Segurança eletrónica

P:  1

#### A3.a - Segurança das Redes e Sistemas de Informação (RSI)

P:  1

1 - A arquitectura de segurança das RSI existentes na U/E/O satisfaz os requisitos técnicos mínimos definidos na Resolução do Conselho de Ministros (RCM) n.º 41/2018, de 22 de março?

Av:  P:  3

2 - Os servidores, sistemas de gestão de redes, controladores de rede e de comunicações, routers, firewalls - referentes a redes e sistemas de informação que tratam dados pessoais - estão localizados em áreas de segurança claramente identificadas e acoplados em bastidores robustos, protegidos e acessíveis apenas com chave?

Av:  P:  2

3 - As estações de trabalho dos utilizadores, em especial as que contenham ou possam ter acesso a dados pessoais críticos, estão localizadas em áreas seguras?

Av:  P:  1

4 - As cablagens das RSI que processam dados pessoais são de fibra ótica ou, em alternativa, distam, no mínimo, de 10 cm das restantes redes filares (i.e. energia elétrica, telefones, dados, etc.) da U/E/O?

Av:  P:  1

5 - O Cmdt/Dir/Ch da U/E/O tem zelado pelo cumprimento da determinação em 4.j.(3) da Diretiva N.º 52/CEME/19, de 27FEV19?

Av:  P:  2

6 - Não existem no interior das áreas de segurança da U/E/O outras linhas de transmissão, equipamentos e dispositivos eletrónicos que não tenham sido prévia e especificamente autorizados pelo Cmdt/Dir/Ch?

Av:  P:  1

7 - Existem e são cumpridos pela U/E/O os normativos e disposições de segurança superiormente aprovados e em vigor, relativamente à interdição de porte e uso de telemóveis, smartphones e outros dispositivos eletrónicos com capacidade fotográfica, no interior das áreas de segurança e restritas?

Av:  P:  1

8 - Existem junto à entrada das áreas de segurança e restritas da U/E/O, letreiros, painéis de aviso, sinalética, pessoal postado, para informar o pessoal que ali afluí da interdição relativa aos equipamentos eletrónicos em vigor, bem como cacifos/locais destinados à sua deposição?

Av:  P:  1

### A4 - Documentação estruturante do Exército

P:  1

#### A4.a - Política de Privacidade do Exército

P:  1

1 - Existe e é do conhecimento do pessoal da U/E/O?

Av:  P:  2

#### A4.b - Código de Conduta do Exército no âmbito da Proteção de Dados

P:  1

1 - Existe e é do conhecimento do pessoal da U/E/O?

Av:  P:  2

#### A4.c - Diretiva de Proteção de Dados do Responsável pelo Tratamento (RT)

P:  1

1 - Existe e é do conhecimento do pessoal da U/E/O?

Av:  P:  2

#### A4.d - Manual de Procedimentos de Proteção de Dados do Exército

P:  1

1 - Existe e o seu conteúdo é do conhecimento do pessoal da U/E/O?

Av:  P:  2

#### A4.e - Modelo de briefing de Proteção de Dados do Exército

P:  1

1 - Existe um briefing tipificado do Exército sobre Proteção de Dados a ministrar ao pessoal da U/E/O?

Av:  P:  2

### A5 - Documentação enquadrante do escalão superior

P:  1

#### A5.a - Diretiva de Proteção de Dados do escalão superior

P:  1

1 - Existe e o seu conteúdo é do conhecimento do pessoal da U/E/O?

Av:  P:  2

2 - A diretiva exprime claramente a intenção e conceito do escalão superior relativamente à Proteção de Dados?

Av:  P:  2

**A6 - Orientações, Diretivas e NEP da U/E/O e Formulários de Proteção de Dados.**P: **A6.a - Orientações do Cmdt/Dir/Ch para a Proteção de Dados na U/E/O**P: 

1 - O Cmdt/Dir/Ch transmitiu orientações claras (verbais e/ou escritas) aos seus subordinados para as questões de Proteção de Dados emergentes na U/E/O?

Av: P: **A6.b - Diretiva de Proteção de Dados do Cmdt/Dir/Ch da U/E/O**P: 

1 - Existe, é esclarecedora, é do conhecimento do pessoal da U/E/O e está atualizada?

Av: P: **A6.c - NEP de Proteção de Dados da U/E/O**P: 

1 - Existe, está convenientemente estruturada, é esclarecedora, está atualizada e é do conhecimento do pessoal da U/E/O?

Av: P: **A6.d - Formulários de Proteção de Dados**P: 

1 - Existe na U/E/O um formulário normalizado de Declaração de Consentimento, em formato digital (template) ou impresso?

Av: P: 

2 - Existe na U/E/O um formulário normalizado de Declaração de Retirada de Consentimento, em formato digital (template) ou impresso?

Av: P: 

3 - Existe na U/E/O um formulário normalizado de Registo de Atividades de Tratamento de dados pessoais, em formato digital (template) ou impresso?

Av: P: 

4 - Existe na U/E/O um formulário normalizado para relato de ocorrências/incidentes, pedidos de esclarecimento e/ou de exercício de direitos pelos titulares de dados pessoais, em formato digital (template) ou impresso?

Av: P: 

5 - Existe na U/E/O um formulário normalizado para Notificação de Violação de Dados Pessoais (Personal Data Breach) para o EPD ou o RT?

Av: P: 

6 - Existe na U/E/O um formulário normalizado para Comunicação de Violação de Dados Pessoais para o Titular dos dados?

Av: P: 

7 - Está disponível na U/E/O um formulário normalizado para Avaliação do Impacto sobre Proteção de Dados (AIPD)?

Av: P: **A7 - Sistema de Informação e de Gestão de Proteção de Dados**P: **A7.a - Gestão da Proteção de Dados**P: 

1 - A U/E/O dispõe de algum software específico, ou encontra-se a mesma inserida em alguma rede/sistema de informação e de gestão da Proteção de Dados implantada no Exército, vocacionada especialmente para o apoio à ação e tarefas dos RPD/EPD?

Av: P:

**B - FUNCIONAMENTO**P:  1**B1 - Tratamento de Dados Pessoais**P:  1**B1.a - Responsabilidades internas**P:  1

1 - O pessoal identifica corretamente o responsável máximo na U/E/O por tudo o que se refere a dados pessoais?

Av:  P:  3

2 - Estão definidas quais as entidades/organismos na U/E/O especificamente autorizados a recolher dados pessoais?

Av:  P:  2

3 - Estão definidas quais as entidades/organismos na U/E/O especificamente autorizados a registar, organizar e estruturar dados pessoais?

Av:  P:  2

4 - Estão definidas quais as entidades/organismos na U/E/O especificamente autorizados a conservar ou armazenar dados pessoais?

Av:  P:  2

5 - Estão definidas quais as entidades/organismos na U/E/O especificamente autorizados a adaptar ou alterar dados pessoais?

Av:  P:  2

6 - Estão definidas quais as entidades/organismos na U/E/O especificamente responsáveis pela execução de cópias de segurança (backups) e recuperação de dados pessoais?

Av:  P:  2

7 - Estão definidas quais as entidades/organismos na U/E/O especificamente autorizados a consultar e utilizar dados pessoais?

Av:  P:  2

8 - Estão definidas quais as entidades/organismos na U/E/O especificamente autorizados a partilhar, disponibilizar ou transmitir (interna ou externamente) dados pessoais?

Av:  P:  2

9 - Estão definidas quais as entidades/organismos na U/E/O especificamente responsáveis pelo apagamento ou destruição dos dados pessoais?

Av:  P:  2**B1.b - Categorias especiais de dados pessoais e informações a facultar**P:  1

1 - A U/E/O realiza tratamento de dados pessoais sensíveis, atentas as situações especiais enumeradas no art.º 9., §2., alíneas de a) a j)?

Av:  P:  2

2 - A U/E/O realiza tratamento de dados pessoais de menores de 16 anos?

Av:  P:  2

3 - O pessoal da U/E/O que lida com dados pessoais, tem conhecimento das disposições legais que regem o seu tratamento e da necessidade de cumprir as mesmas?

Av:  P:  2

4 - A U/E/O, através do RPD, diligencia, por norma, no sentido de prestar aos titulares as informações a que se referem os art.º 13.º e 14.º do RGPD, bem como qualquer comunicação prevista nos art.º 15.º a 22.º e 23.º do RGPD, a respeito do tratamento de dados pessoais, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, quer por escrito, quer por outros meios, inclusive eletrónicos?

Av:  P:  2**B1.c - Risk assessment**P:  1

1 - A U/E/O empreendeu uma prévia apreciação dos riscos (risk assessment) associados ao tratamento de dados pessoais?

Av:  P:  2**B1.d - Princípios relativos ao tratamento de dados pessoais**P:  1

1 - O tratamento dos dados pessoais na U/E/O é lícito (p. ex. sustentado na lei, no consentimento, no cumprimento dos termos da celebração de um contrato, na defesa dos interesses vitais do titular ou de terceiro, entre outros), leal e transparente (i. e. com informação clara, concisa e de modo compreensível ao titular dos riscos, regras e seus direitos)?

Av:  P:  1

2 - Os dados pessoais são tratados na U/E/O para fins específicos, explícitos e legítimos, o que pressupõe obrigatoriedade de informação ao titular, não podendo aqueles ser a posteriori tratados de forma distinta e incompatível com tais fins?

Av:  P:  1

3 - Os dados pessoais na U/E/O são adequados, pertinentes e limitados ao necessário, sendo apenas considerados os relevantes e estritamente suficientes para o cumprimento das finalidades para as quais são tratados?

Av:  P:  1

4 - Os dados pessoais que são objeto de tratamento na U/E/O, são exatos e atualizados sempre que necessário, existindo procedimentos instituídos para verificar a sua correção e validade, bem como para prontamente os retificar/apagar quando inexatos?

Av:  P:  1



5 - Os dados pessoais na U/E/O são conservados apenas durante o tempo necessário à consecução das finalidades para as quais são tratados, existindo prazos definidos para a sua conservação e procedimentos instituídos para o seu arquivo/destruição?

Av:  P:  1

6 - Os dados pessoais na U/E/O são tratados de forma segura, protegidos contra acessos e tratamentos não autorizados ou ilícitos e contra perdas acidentais, danos ou destruição?

Av:  P:  1

7 - A U/E/O aplica medidas organizativas e técnicas a fim de garantir a segurança dos dados e a proteção contra acessos e tratamentos indevidos/ilícitos, designadamente, a pseudonimização?

Av:  P:  1

8 - A par da responsabilidade que lhe incumbe pelo cumprimento dos princípios relativos ao tratamento de dados pessoais, o Cmdt/Dir/Ch da U/E/O está ciente de que deverá ser capaz de comprová-lo?

Av:  P:  1

#### B1.e - Licitude do tratamento

P:  1

1 - A U/E/O justifica a licitude do tratamento de dados pessoais, à luz das situações tipificadas no n.º 1 do art.º 6.º do RGPD?

Av:  P:  1

2 - A U/E/O justifica a licitude do tratamento de dados pessoais sensíveis, se aplicável, à luz das situações tipificadas no n.º 2 do art.º 9.º do RGPD?

Av:  P:  1

3 - No caso de a licitude do tratamento se basear no consentimento, inequívoco ou explícito, do titular para uma ou mais finalidades específicas, o Cmdt/Dir/Ch da U/E/O está ciente de que deverá ser capaz de demonstrá-lo ?

Av:  P:  2

#### B1.f - Consentimento

P:  1

1 - O texto do formulário de Declaração de Consentimento está expresso de modo inteligível e em linguagem clara e simples, a sua assinatura/preenchimento é de antemão solicitada aos titulares dos dados pessoais e, no caso de menores de 16 anos, aos respetivos titulares das responsabilidades parentais?

Av:  P:  1

2 - O Cmd/Dir/Ch da U/E/O está ciente de que deverá ser capaz de demonstrar que o consentimento é dado livremente pelo titular dos dados/titular das responsabilidades parentais, que a execução das tarefas/ações subsequentes não fica subordinada à sua concessão e que esse acto fica registado na U/E/O, sob controlo do respetivo RPD?

Av:  P:  2

3 - Pode o titular dos dados, em qualquer momento e com facilidade, mediante o preenchimento de um formulário para o efeito, retirar o seu consentimento e foi o mesmo informado deste direito, previamente à concessão do referido consentimento?

Av:  P:  1

#### B1.g - Tratamento

P:  1

1 - A U/E/O realiza o tratamento de dados pessoais por meios total ou parcialmente automatizados, ou através de meios não automatizados, sendo os dados pessoais contidos em ficheiros?

Av:  P:  1

2 - Através do ARL em coordenação com o RPD, é mantido um estrito controlo dos ficheiros, arquivos físicos e digitais e bases de dados pessoais correntes e em uso nos sistemas de informação em rede, dispositivos móveis e equipamentos stand-alone existentes na U/E/O, em função da sua criticidade, necessidade e licitude, à luz do RGPD?

Av:  P:  2

3 - Através do RPD, a U/E/O mantém um registo de todas as atividades de tratamento de dados sob sua responsabilidade?

Av:  P:  2

4 - A natureza, âmbito e finalidade do tratamento de dados pessoais exigem que a U/E/O proceda a um controlo regular e sistemático dos titulares dos dados, em grande escala?

Av:  P:  1

5 - A U/E/O tem necessidade de definir perfis?

Av:  P:  1

6 - A definição de perfis de titulares utiliza dados pessoais sensíveis?

Av:  P:  1

7 - A definição de perfis de titulares utiliza dados pessoais de menores de 16 anos?

Av:  P:  1

8 - Além do espaço da União Europeia, onde se localiza, a U/E/O tem necessidade de efetuar operações de tratamento de dados para outros territórios?

Av:  P:  1

9 - A U/E/O tem necessidade de executar qualquer tipo de transferência de dados para entidades/organismos situados em países terceiros ou organizações internacionais?

Av:  P:  1

10 - A U/E/O tem necessidade de celebrar protocolos/acordos/memoranda com entidades externas, regulando deveres e obrigações em matéria de tratamento e Proteção de Dados?

Av:  P:  1

**B2 - Direitos dos Titulares dos Dados**P: **B2.a - Direito de acesso**P: 

1 - Existe na U/E/O algum procedimento instituído, a fim de que os titulares possam exercer, junto do RT (através do RPD), o direito de obter a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, em caso afirmativo, o direito de aceder aos seus dados pessoais e às informações enunciadas no art.º 15.º §1.º, alíneas a) a h) do RGPD, sem restrições, sem demoras ou custos excessivos e, por forma a conhecer todas as informações disponíveis acerca da sua origem?

Av: P: 

2 - Subsequente à apreciação e decisão do RT, o RPD da U/E/O foi capaz de providenciar a resposta aos titulares dos dados pessoais, no prazo de 01 mês (02 meses dependendo da complexidade das situações e do volume de pedidos) a contar da data de receção dos pedidos?

Av: P: 

3 - O RPD da U/E/O assegurou convenientemente o registo, gestão e encaminhamento dos pedidos dos titulares, bem como o controlo do cumprimento das decisões do RT?

Av: P: **B2.b - Direito de retificação**P: 

1 - Existe na U/E/O algum procedimento instituído, a fim de que os titulares possam exercer, junto do RT (através do RPD), o direito de obter, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito, ou o completamento dos seus dados pessoais incompletos, tendo os interessados sido devidamente esclarecidos nesse sentido?

Av: P: 

2 - O RPD da U/E/O comunicou oportunamente a cada titular dos dados pessoais a decisão do RT relativamente ao respetivo pedido de retificação/completamento, bem como a ação tomada ou a tomar subsequentemente?

Av: P: 

3 - O RPD da U/E/O assegurou convenientemente o registo, gestão e encaminhamento dos pedidos dos titulares, bem como o controlo do cumprimento das decisões do RT?

Av: P: **B2.c - Direito de apagamento**P: 

1 - Existe na U/E/O algum procedimento instituído, a fim de que os titulares possam exercer, junto do RT (através do RPD), o direito de obter, sem demora injustificada, o apagamento dos seus dados pessoais, quando se verifique um dos motivos explicitados no art.º 17.º §1.º, alíneas a) a f) do RGPD?

Av: P: 

2 - Além dos esclarecimentos prestados pelo RPD acerca do modo como poderão exercer esse direito, os titulares foram informados que o exercício do direito de apagamento ("direito a ser esquecido") pode ser limitado ou restringido em relação ao pessoal militar e civil do Exército?

Av: P: 

3 - O RPD da U/E/O comunicou oportunamente a cada titular dos dados pessoais, a decisão do RT relativamente ao respetivo pedido de apagamento, bem como a ação tomada ou a tomar subsequentemente?

Av: P: 

4 - O RPD da U/E/O assegurou convenientemente o registo, gestão e encaminhamento dos pedidos dos titulares, bem como o controlo do cumprimento das decisões do RT?

Av: P: **B2.d - Direito de limitação do tratamento**P: 

1 - Existe na U/E/O algum procedimento instituído, a fim de que os titulares possam exercer, junto do RT (através do RPD), o direito de obter a limitação do tratamento dos seus dados pessoais, quando se aplique uma das situações previstas no art.º 18.º §1.º, alíneas a) a d) do RGPD?

Av: P: 

2 - O RPD da U/E/O esclareceu os titulares dos dados que, relativamente ao pessoal militar e civil do Exército, a aplicação ou exceção deste direito decorre, forçosamente, de prévia apreciação casuística e que apenas a definição do caso concreto poderá dar a resposta exata, a qual, em função das circunstâncias, poderá ser no sentido da sua aplicabilidade ou no oposto?

Av: P: 

3 - O RPD da U/E/O comunicou oportunamente a cada titular dos dados pessoais a decisão do RT relativamente ao respetivo pedido de limitação do tratamento, bem como a ação tomada ou a tomar subsequentemente?

Av: P: 

4 - O RPD da U/E/O assegurou convenientemente o registo, gestão e encaminhamento dos pedidos dos titulares, bem como o controlo do cumprimento das decisões do RT?

Av: P:



**B2.e - Direito de portabilidade dos dados**P: 

1 - O RPD da U/E/O está ciente de que, por força do estipulado no §3. do art.º 20.º do RGPD, que consagra o tratamento necessário para o exercício de funções de interesse público, o direito de portabilidade dos dados não se afigura, em princípio, extensível ao pessoal militar e civil em serviço no Exército?

Av: P: **B2.f - Direito de oposição**P: 

1 - Existe na U/E/O algum procedimento instituído, a fim de que os titulares possam exercer, junto do RT (através do RPD), o direito de se oporem, a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, com base no art.º 6.º, §1.º, alíneas e) ou f), ou no art.º 6.º, §4.º do RGPD, incluindo a definição de perfis, tendo os interessados sido devidamente esclarecidos nesse sentido?

Av: P: 

2 - Na sequência da decisão do RT, o RPD da U/E/O comunicou a cada titular a cessação do tratamento dos respetivos dados pessoais, ou as razões imperiosas e legítimas prevalecentes sobre os interesses, direitos e liberdades dos titulares dos dados, que ditaram a prossecução desse tratamento?

Av: P: 

3 - O RPD da U/E/O assegurou convenientemente o registo, gestão e encaminhamento dos pedidos dos titulares, bem como o controlo do cumprimento das decisões do RT?

Av: P: **B2.g - Decisões individuais automatizadas, incluído definição de perfis**P: 

1 - Existe na U/E/O algum procedimento instituído, a fim de que os titulares possam exercer, junto do RT (através do RPD), o direito de não serem objeto de uma decisão baseada unicamente no tratamento automatizado, incluindo a elaboração de perfis, que seja suscetível de produzir efeitos jurídicos ou causar quaisquer inconvenientes/danos pessoais?

Av: P: 

2 - Caso exista processamento de dados associados a decisões individuais automatizadas, conforme mencionado no §2.º do art.º 22.º do RGPD, o tratamento de dados para definição de perfis é baseado no consentimento explícito do titular?

Av: P: **B3 - Violação de Dados Pessoais (Personal Data Breach )**P: **B3.a - Investigação sumária**P: 

1 - Perante uma alegada queixa/reclamação de violação de dados pessoais, ou de eventual comprometimento e/ou quebra de segurança de que chegue ao seu conhecimento, o RPD da U/E/O conduziu, de imediato, uma investigação sumária com celeridade, a fim de apurar os factos, as circunstâncias e as causas da ocorrência, bem como aquilatar se a mesma é procedente?

Av: P: **B3.b - Notificação do EPD do Exército**P: 

1 - Subsequentemente, o RPD da U/E/O elaborou e submeteu, no prazo máximo de 48 horas, uma notificação padronizada, por via eletrónica, ao EPD do Exército, dando também conhecimento da ocorrência ao seu canal de Comando?

Av: P: 

2 - Caso a notificação para o EPD não tenha sido transmitida no prazo de 48 horas, o RPD da U/E/O anexou, por escrito, os motivos desse atraso?

Av: P: **B3.c - Comunicação de violação de dados pessoais ao titular**P: 

1 - Existe na U/E/O um procedimento estabelecido para, sem demora injustificada, se efetuar a comunicação de violação de dados pessoais aos respetivos titulares de dados, quando tal for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares?

Av: P: **B3.d - Registo de incidentes de segurança e violações de dados pessoais**P: 

1 - O RPD da U/E/O mantém um registo atualizado das queixas, reclamações e de comprovadas violações de dados pessoais ocorridas, bem como das circunstâncias, dos efeitos e das inerentes decisões e medidas corretivas adotadas?

Av: P: **B3.e - NEP de Resposta a Incidentes de Segurança e Proteção de Dados**P: 

1 - A U/E/O dispõe de uma NEP específica de resposta a incidentes de segurança e proteção de dados, cujos procedimentos são exercitados, revistos e atualizados, com regularidade?

Av: P:

**B4 - Publicitação de contratos públicos na área pública do Portal BASE**  
(<https://www.base.gov.pt/base4>)P: **B4.a - Expurgo dos dados pessoais dos contratos públicos publicados/a publicar**P: 

1 - O Cmdt/Dir/Ch está ciente que a publicação no Portal BASE dos contratos públicos eventualmente celebrados pela U/E/O, deve ser previamente expurgada de todos os dados pessoais neles constantes, com exceção da identificação do contraente público ou entidade adjudicante, do cocontratante ou adjudicatário e do gestor de contrato?

Av: P: 

2 - Todos os contratos públicos eventualmente celebrados pela U/E/O e publicados no Portal BASE apresentam o expurgo dos dados pessoais, conforme superiormente determinado, com a exceção do nome das entidades intervenientes?

Av: P: 

3 - Nos contratos públicos eventualmente celebrados pela U/E/O e publicados no Portal BASE, foi utilizada uma ferramenta tecnológica/metodologia que assegura eficazmente a ocultação e/ou a extração dos dados pessoais que foram previamente expurgados?

Av: P: **B5 - Avaliação de Impacto sobre a Proteção de Dados**P: **B5.a - Apoio e contributos da U/E/O para as AIPD**P: 

1 - O Cmd/Dir/Ch da U/E/O e/ou o seu RPD estão cientes e capacitados para prestar apoio e colaboração, quando necessário, mediante a produção de contributos relevantes para a realização das avaliações de impacto sobre a proteção de dados (AIPD ou DPIA) que sejam determinadas pelo RT, quando se perspetivar que um certo tipo de tratamento, em particular, que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares?

Av: P: