Esta obrigatoriedade decorre da importância dos resultados do Recenseamento Agrícola para a definição e monitorização da Política Agrícola Comum, cuja relevância se encontra traduzida ao nível do orçamento da UE, enquanto instrumento fundamental para o desenvolvimento económico e social europeu.

O Recenseamento Agrícola constitui um instrumento essencial para o conhecimento da agricultura portuguesa, para a quantificação do seu contributo para a economia nacional, para a definição das políticas públicas e para a tomada de decisão no domínio privado deste setor.

Estas valências são particularmente relevantes para o sucesso da aposta formulada no Programa do XXI Governo Constitucional, tendo em vista a dinamização do setor agrícola português, o qual tem captado o interesse crescente de jovens empreendedores, quer por via de apoios para a instalação da atividade, quer mediante o uso cada vez mais frequente de novas tecnologias, quer ainda através da valorização da agricultura e da sua cada vez mais importante contribuição para o aumento das exportações nacionais.

Nesse sentido, é criada uma Comissão de Acompanhamento com a missão de acompanhar a preparação e a implementação do Recenseamento Agrícola 2019, cuja coordenação é assegurada pelo Instituto Nacional de Estatística, I. P., enquanto entidade responsável pela realização do Recenseamento Agrícola, em articulação com o Gabinete de Planeamento, Políticas e Administração Geral, a quem cabe organicamente assegurar a coordenação da produção de informação estatística no âmbito da área governativa da Agricultura, Florestas e Desenvolvimento Rural, e que integra ainda na sua composição os serviços, organismos e estruturas representativas relevantes neste domínio, sendo de destacar, ao nível operacional, a atuação das Direções Regionais de Agricultura e Pescas, em particular nos trabalhos de recolha da informação.

Assim:

Nos termos da alínea *g*) do artigo 199.º da Constituição, o Conselho de Ministros resolve:

1 — Criar a Comissão de Acompanhamento do Recenseamento Agrícola 2019 (RA2019), adiante designada por Comissão, com a missão de acompanhar o desenvolvimento, preparação e a implementação do RA2019.

2 — Estabelecer que a Comissão é coordenada pelo Instituto Nacional de Estatística, I. P. (INE, I. P.), em articulação com o Gabinete de Planeamento, Políticas e Administração Geral (GPP), sendo composta por um representante dos seguintes serviços, organismos e estruturas representativas:

a) Direção-Geral de Agricultura e Desenvolvimento Rural;
b) Direção-Geral de Alimentação e Veterinária;
c) Instituto da Conservação da Natureza e das Florestas, I. P.;
d) Instituto de Financiamento da Agricultura e Pescas, I. P.;
e) Direções Regionais de Agricultura e Pescas;
f) Agência Portuguesa do Ambiente, I. P.;
g) Associação Nacional de Municípios Portugueses;
h) Associação Nacional de Freguesias.

3 — Determinar que integram ainda a Comissão a Direção Regional de Estatística da Madeira e o Serviço Regional de Estatística dos Açores, na qualidade de responsáveis pela articulação com os serviços regionais competentes.

4 — Estabelecer que a Comissão pode convidar outras entidades a participar nas suas reuniões, em função das matérias em agenda, designadamente a Autoridade de Gestão do Programa de Desenvolvimento Rural do continente (PDR2020), a Direção-Geral de Energia e Geologia, a Direção-Geral do Território e as organizações socioprofissionais do setor agrícola.

5 — Estabelecer que as entidades referidas no n.º 2 designam os seus representantes no prazo máximo de 10 dias a contar da publicação da presente resolução, sendo a respetiva designação comunicada ao INE, I. P.

6 — Determinar que compete à Comissão:

a) Colaborar na definição do Plano Global da Operação, mediante proposta do INE, I. P.;
b) Cooperar com o INE, I. P., na definição do plano de trabalhos que concretize as ações a realizar pelas entidades envolvidas, a respetiva calendarização e os recursos a afetar;
c) Apoiar na inventariação e priorização das necessidades de informação estrutural agrícola;
d) Analisar os aspetos técnicos relevantes para a formulação do questionário a utilizar no RA2019 e respetivos conceitos a adotar;
e) Colaborar na definição do universo de explorações agrícolas a inquirir;
f) Apoiar na definição da estrutura orgânica e funcional de recolha de informação a elaborar pelo INE, I. P.;
g) Contribuir para a definição do quadro de formação dos intervenientes na operação;
h) Colaborar na análise e divulgação dos resultados do RA 2019;
i) Apoiar a execução do plano de comunicação institucional, a elaborar pelo INE, I. P., e participar em ações de divulgação.

7 — Prever que o apoio logístico e administrativo necessário ao funcionamento da Comissão é assegurado pelo INE, I. P.

8 — Estabelecer que as Direções Regionais de Agricultura e Pescas disponibilizam instalações destinadas a funcionar como centros de recolha, em colaboração com as estruturas representativas referidas nas alíneas *g*) e *h*) do n.º 2, bem como para o desenvolvimento de outras atividades associadas à operacionalização da operação.

9 — Estabelecer que os encargos decorrentes do RA2019 são suportados por dotação constante do orçamento do INE, I. P., inscrita e a inscrever, e por subvenção da Comissão Europeia.

10 — Determinar que a presente resolução entra em vigor no dia seguinte ao da sua publicação.

Presidência do Conselho de Ministros, 22 de março de 2018. — Pelo Primeiro-Ministro, *Augusto Ernesto Santos Silva,* Ministro dos Negócios Estrangeiros.

111231535

Resolução do Conselho de Ministros n.º 41/2018

O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, doravante designado RGPD, veio introduzir um novo regime em matéria de proteção de dados pessoais, tendo revogado a Diretiva n.º 95/46/CE.

Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD exige novas regras e procedimentos do ponto de vista tecnológico.

A relação entre a tecnologia e o Direito está espelhada, de modo especial, na proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD), nas medidas adequadas para garantir a segurança do tratamento (artigo 32.º do RGPD), na notificação de violações de dados pessoais às autoridades de controlo (artigo 33.º do RGPD), na comunicação de violação de dados pessoais aos titulares dos dados (artigo 34.º do RGPD) e na avaliação de impacto sobre a proteção de dados (artigo 35.º do RGPD).

O direito ao apagamento dos dados pessoais e o direito à portabilidade destes, consagrados respetivamente nos artigos 17.º e 20.º do RGPD, exigem igualmente a implementação de tecnologias de informação que utilizem formatos interoperáveis, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, e que permitam que estes direitos possam ser efetivamente exercidos.

Nesta medida, o Governo considera fundamental definir orientações técnicas para a Administração Pública, recomendando-as ao setor empresarial do Estado, em matéria de arquitetura de segurança das redes e sistemas de informação e procedimentos a adotar de modo a cumprir as normas do RGPD.

Tendo em conta que o RGPD é aplicável a partir de 25 de maio de 2018, cumpre desde já fixar as mencionadas orientações.

Assim:

Nos termos da alínea *g*) do artigo 199.º da Constituição, o Conselho de Ministros resolve:

1 — Aprovar os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, os quais constam do anexo à presente resolução e que dela faz parte integrante.

2 — Recomendar a aplicação dos requisitos técnicos a que se refere o número anterior também nas redes e sistemas de informação do setor empresarial do Estado.

3 — Determinar que cada serviço e entidade da Administração direta e indireta do Estado deve avaliar a conformidade dos requisitos técnicos das redes e sistemas de informação em uso com as finalidades e princípios de segurança que se pretendem alcançar com os requisitos estabelecidos no anexo à presente resolução.

4 — Determinar que os requisitos referidos no anexo à presente resolução devem ser implementados no prazo máximo de 18 meses após a data de entrada em vigor da presente resolução.

5 — Estabelecer que a presente resolução entra em vigor no dia seguinte ao da sua publicação.

Presidência do Conselho de Ministros, 22 de março de 2018. — Pelo Primeiro-Ministro, *Augusto Ernesto Santos Silva,* Ministro dos Negócios Estrangeiros.

ANEXO

(a que se referem os n.os 1, 3 e 4)

Arquitetura de segurança das redes e sistemas de informação

Requisitos técnicos

Notas:

FE — *Front-end*;
App — Camada Aplicacional
BD — Camada de Base de Dados

Requisito geral	Requisitos Específicos		Classificação
As aplicações cliente (exemplo, *Android,* IOS, WEB) devem ser desenvolvidas adotando práticas de desenvolvimento seguro.	FE	Seguir as boas práticas de desenvolvimento. Exemplo: *Open Web Application Security Project* (OWASP), no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança.	Obrigatório.
		Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.
		Recomenda-se o uso de *Transport Layer Security* (TLS), na sua versão mais recente.	Recomendado.
		Não guardar informação pessoal no *browser*, memória ou disco, para além do tempo da sessão e apenas na medida do necessário.	Obrigatório.
	App	Utilização de sessões seguras com protocolo de Segurança.	Obrigatório.
		Recomenda-se o uso de TLS, na sua versão mais recente, na comunicação com as camadas adjacentes.	Recomendado.
		Se possível usar certificados através de *Application Programming Interface* (API), não sendo desta forma necessário o uso de palavras-passe.	Recomendado.
		Não é permitida a utilização de credenciais em *plain text*, quer no código quer em ficheiros de configuração	Recomendado.
		Deve ser evitado palavras-passe embebidas no código.	Recomendado.
		As credenciais que necessitem de ser armazenadas em ficheiros de configuração devem estar codificadas (HASH — mínimo SHA 256).	Recomendado.
	BD	Comunicação com camada aplicacional através de autenticação por certificado válido por período não superior a 2 anos, no caso de as camadas serem física ou logicamente distintas.	Obrigatório.
		Exemplo: padrão X.509, da ITU-T para Infraestruturas de Chaves Públicas (ICP).	
		Prever cifra de informação pessoal (recomenda-se mínimo 2048 bit) apenas se a aplicação cliente tiver camada de BD física e logicamente distinta, usando preferencialmente tecnologia que permita interoperabilidade entre sistemas.	Obrigatório.

Requisito geral	Requisitos Específicos		Classificação
Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso a sistemas e aplicações.	FE	O processo de autenticação deve ser sempre iniciado e mantido em sessão segura.	Obrigatório.
		Recomenda-se: 1) o uso de TLS, na sua versão mais recente; ou 2) o uso de palavra-passe, preferencialmente em combinação com outro fator (*Double Factor Authentication*-2FA), como por exemplo: Palavra-passe + SMS *Token* Palavra-passe + *Smartcard* Palavra-passe + Biometria Palavra-passe + padrão gráfico Palavra-passe + Cartão de coordenadas Palavra-passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR-*Code*.	Recomendado.
		Dados pessoais de sessão excluídos das variáveis *Uniform Resource Locator* (URL) ou de outras variáveis visíveis ao utilizador.	Obrigatório.
		Credenciais de início de sessão transmitidos através do seu HASH, mínimo *Secure Hash Algorithm*-256 (SHA-256), ou utilização de cifra ou codificação para a transmissão de dados pessoais (nome do utilizador e palavra-passe em HASH e restantes dados cifrados).	Obrigatório.
		Sempre que aplicável, a palavra-passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório.
		Recomenda-se que para novos sistemas seja sempre usado como padrão de autenticação o 2FA.	Recomendado.
	App	A palavra-passe dos administradores deve ter no mínimo 13 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório.
		Para todos os administradores deve-se utilizar Padrão de autenticação 2FA: Exemplos: Palavra-passe + *Smartcard* Palavra-passe + Biometria Palavra-passe + certificado (por exemplo X.509, da ITU-T para ICP, válido por período não superior a 2 anos).	Obrigatório.
		Como mecanismo de proteção e segurança da informação recomenda-se o uso de *Token*.	Recomendado.
		Comunicação com camadas FE ou BD através de sessão segura, com prévia autenticação se camadas forem física ou logicamente distintas.	Obrigatório.
		Deve ser evitado palavras-passe embebidas no código. Quando tal não for possível, devem estar codificadas (HASH, mínimo SHA-256).	Recomendado.
		Se possível, usar certificados através de API, não sendo desta forma necessário o uso de palavras-passe.	Recomendado.
		Autenticação de elementos comunicantes garantida por validação de informação estática ao nível da rede. Exemplos: 1) utilização de IP fixo + *hostname* + *MacAddress* + fatores de autenticação, ou 2) Utilização de certificados.	Obrigatório.
	BD	A palavra-passe deve ter no mínimo 13 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a...z), letras maiúsculas (A...Z), números (0...9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /). Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».	Obrigatório.
		Dados pessoais de autenticação, transmitidos através do seu HASH (mínimo SHA-256), ou recorrendo à cifra ou codificação para efetuar essa transmissão.	Recomendado.

Requisito geral	Requisitos Específicos		Classificação
Atribuição de direitos de acesso e privilégio de forma restrita e controlada.	FE	Criação de perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (*Create, Read, Update, Delete* — CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Criação de registo de acesso, alteração e remoção (*logs*), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.
	App	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Criação de registo de acesso, alteração e remoção (*logs*) com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.
	BD	Criação perfis com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Criação de registo de acesso, alteração e remoção (*logs*), com informação sobre quem acedeu, de onde acedeu (IP e Porto), quando acedeu, a que dados acedeu, que ação foi efetuada sobre os mesmos (CRUD).	Obrigatório.
Atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida.	FE	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.
		Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação. Exemplo: Envio de informação de autenticação por SMS com validade limitada (não superior a 5 minutos), com primeiro acesso a implicar sempre a redefinição da informação enviada; Envio de informação de autenticação gerada automática e aleatoriamente, enviada por Envelope (semelhante ao do envio de dados do Cartão de Cidadão).	Obrigatório.
	App	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.
		Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório.
	BD	Processo definido de acordo com a política de «Atribuição de direitos de acesso e privilégio de forma restrita e controlada».	Obrigatório.
		Atribuição de credenciais de acesso efetuada de forma a permitir a sua auditoria, sem permitir outro acesso que não o do destinatário da informação.	Obrigatório.
Revisão de direitos de acesso de utilizadores em intervalos regulares.	FE	Processo de renovação de conta do utilizador de acordo com os mesmos requisitos de segurança da criação do mesmo, não devendo ter um ciclo de vida superior a 180 dias.	Obrigatório.
		A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.
		Deve ser desativada uma conta de utilizador quando o mesmo não tem atividade sobre a conta durante 3 meses.	Recomendado.
	App	Processo de gestão de validade de perfis.	Obrigatório.
		Processo de gestão de validade de perfis automatizado.	Recomendado.
		Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.

Requisito geral	Requisitos Específicos		Classificação
	BD	Processo de gestão de validade de perfis.	Obrigatório.
		Processo de gestão de validade de perfis automatizado.	Recomendado.
		Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade, no máximo bimestral ou quando se verifique uma alteração no mapa de pessoal associado a esta função.	Obrigatório.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.
Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados.	FE	A gestão do ciclo de vida da conta do utilizador deve ter em conta a segregação das funções existentes e os privilégios de acesso que devem estar associados a essas funções, em cada momento (privilégios mínimos, onde cada tipo de conta de utilizador é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.
		Ação dos utilizadores sobre dados pessoais (CRUD) deve permitir a sua auditoria em registo de atividade (*logs*).	Obrigatório.
	App	Para Administradores de Sistemas, Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.
		Processo de gestão de validade de contas de utilizadores.	Obrigatório.
		Processo de gestão de validade de contas de utilizadores automatizado.	Recomendado.
		Processo automatizado ou interoperável com sistemas responsáveis pela gestão das funções associados aos privilégios atribuídos a cada perfil. Em casos de verificação assíncrona do binómio função/privilégios, a mesma deve ocorrer com uma periodicidade limitada.	Obrigatório.
		Recomenda-se: 1) uma periodicidade bimestral; ou 2) quando se verifique uma alteração no mapa de pessoal associado a esta função.	Recomendado.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.
	BD	Para Administradores de Bases de Dado, Administradores de Sistemas, de Redes e Aplicacional, caso acedam a dados pessoais, aplicam-se os requisitos da camada FE.	Obrigatório.
		Processo de gestão de validade das contas dos utilizadores.	Obrigatório.
		Processo de gestão de validade das contas dos utilizadores automatizado.	Recomendado.
		Alarmística para contas de utilizadores sem atividade registada durante um período superior a 3 meses.	Recomendado.
Restrição de acesso à informação baseado no princípio necessidade de conhecer (criação de perfil).	FE	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
	App	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório.
	BD	Associação da tipologia de dados a perfis específicos, individuais e associados à função, com privilégios mínimos, onde cada tipo de perfil é definido em função do Tipo de Dado Pessoal a que acede e Ação que pode efetuar sobre o Dado Pessoal (CRUD), de acordo com o princípio da necessidade de conhecer.	Obrigatório.
		Processo de registo de tentativas de acesso a dados excluídos dos privilégios associados ao perfil (qualquer perfil, incluindo o dos administradores), com alarmística a partir de um determinado número de tentativas (por exemplo, 3 tentativas), a notificar ao encarregado da proteção de dados da organização.	Obrigatório.

Requisito geral	Requisitos Específicos		Classificação
Automatização dos processos de concessão, revisão, análise e revogação de acesso.	Aplicam-se as mesmas disposições que em «Capacidade para garantir que os utilizadores fazem uma utilização correta dos dados» e «Revisão de direitos de acesso de utilizadores em intervalos regulares».		Obrigatório.
Procedimentos seguros de início de sessão.	Aplicam-se as mesmas disposições referidas em «Capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o acesso controlado por um procedimento seguro de início de sessão».		Obrigatório.
Capacidade de monitorização, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis.	Deve ser guardado registo de atividade (*log*) de todas as ações que um utilizador efetue sobre dados pessoais, independentemente do seu perfil e função.		Obrigatório.
	Todos os registos de atividade (*log*) devem ser armazenados apenas em modo de leitura, devendo, com uma periodicidade máxima de 1 mês, ser englobados num único bloco de registos e assinado digitalmente (garantia de integridade).		Obrigatório.
	Deve ser guardado registo de atividade (*log*) de todos os acessos e tentativas falhadas de acesso, obedecendo aos requisitos anteriores.		Obrigatório.
	Garantir que os registos de atividade provenientes dos diversos subsistemas (Sistemas Operativos, aplicações, *browsers*, Sistema de Gestão de Base de Dados — SGBD, etc.) são inequivocamente associados à sua origem.		Obrigatório.
	Os registos de atividade (*log*) devem conter, no mínimo, o endereço de acesso (IP e Porto), *Host*, HASH da conta do utilizador que efetuou a ação, ação efetuada (CRUD), Tipo de Dado Pessoal onde a ação foi efetuada, data/hora/minuto/segundo (*TimeStamp*) da ação, alteração efetuada sobre o dado pessoal.		Obrigatório.
Inspeção automática dos conteúdos para procurar dados sensíveis e acessos remotos ao sistema a partir do exterior do ambiente organizacional.	Tendo em vista garantir que a entidade responsável pelo tratamento de dados deve definir e implementar mecanismos de proteção da informação em função da sua relevância e criticidade, deve ser implementado: Deteção de ameaças na defesa perimétrica do sistema (por exemplo, regras definidas nas *firewall*, *Intrusion Detection System* — IDS, etc.); Extensão desta proteção desejavelmente a todos os dispositivos (incluindo móveis) com acesso a dados pessoais nos sistemas corporativos; Mecanismo de cifra ponto a ponto sempre que houver necessidade de aceder remotamente ao FE (e apenas a esta camada), como por exemplo com recurso à tecnologia *Virtual Private Network* (VPN).		Obrigatório.
Proteção dos dados contra modificações não autorizadas, perdas, furtos e divulgação não autorizada.	FE	FE desenvolvido e em produção de acordo com as melhores práticas de segurança, garantindo a proteção desta camada aos ataques mais comuns (SQLi, injeção de código, etc.).	Obrigatório.
		Recomenda-se as práticas recomendadas em *Open Web Application Security Project* (OWASP).	Recomendado.
		Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.
	App	Camada aplicacional segregada da rede ou ambiente com visibilidade e/ou acesso exterior.	Obrigatório.
		Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.
	BD	Camada de BD segregada da rede ou ambiente com visibilidade/acesso exterior.	Obrigatório.
		Aplicam-se as disposições anteriores relativas à segurança da atribuição dos acessos e segurança dos dados pessoais, dos acessos propriamente ditos e do registo da atividade efetuada sobre os dados pessoais.	Obrigatório.
		Mascaramento, anonimização ou, sendo necessário, cifra dos dados pessoais transmitidos ou acedidos.	Obrigatório.
		Dados armazenados (incluindo os existentes em volumes de salvaguarda — *backups*) devem ser cifrados e assinados digitalmente.	Recomendado.
		Recomenda-se que, para dados pessoais considerados muito críticos, o seu armazenamento seja efetuado de forma fragmentada e em locais físicos distintos, mantendo-se todavia a sua unicidade e integridade lógica.	Recomendado.
Capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais.	Deve ser garantida a integridade das zonas *Domain Name System* (DNS) onde se encontra inserido o sistema e o ecossistema envolvente, recorrendo às boas práticas de DNSSec e de configuração de sistemas de Correio Eletrónico (por exemplo, *Sender Policy Framework* — SPF, *DomainKeys Identified Mail* — DKIM, *Domain-based Message Authentication*, *Reporting and Conformance* — DMARC, entre outros).		Obrigatório.

Requisito geral	Requisitos Específicos	Classificação
	Deve ser utilizada tecnologia de comunicação segura (por exemplo VPN), com sistema de autenticação forte (preferencialmente através de certificados), para que a transmissão de dados entre entidades de ambientes tecnológicos distintos seja efetuada em segurança.	Recomendado.
Os sistemas de armazenamento devem garantir redundância e disponibilidade, não devendo existir nenhum «single point of failure».	A arquitetura de processamento e armazenamento deve garantir as propriedades da redundância, resiliência e disponibilidade.	Obrigatório.
	Devem existir dois tipos de *backups* (*online* e *offsite*), que devem obedecer aos mesmos requisitos de segurança definidos para os sistemas produtivos.	Obrigatório.
	Os *backups offsite* devem ser guardados numa localização que não esteja exposta aos mesmos riscos exteriores da localização original, podendo ser da organização mas geograficamente distinta e/ou afastada.	Obrigatório.
As redes e sistemas de informação devem possuir as funcionalidades necessárias ao respeito pelos direitos do titular dos dados.	Os sistemas devem estar capacitados para classificar, priorizar, pesquisar, editar e apagar os dados pessoais.	Obrigatório.
	Os sistemas devem possuir os controlos necessários que permitam a identificação, autenticação, acesso e validação dos dados pessoais armazenados.	Obrigatório.
As tecnologias de informação a implementar devem permitir a portabilidade e a exportação de dados pessoais.	Deve-se garantir a utilização de formatos digitais compatíveis, que assegurem a interoperabilidade técnica e semântica dentro da Administração Pública, na interação com o cidadão ou com a empresa e para disponibilização de conteúdos e serviços, adotando as especificações técnicas e formatos digitais definidos no Regulamento Nacional de Interoperabilidade Digital, aprovado pela Resolução do Conselho de Ministros n.º 91/2012, ou noutro que o venha a substituir.	Obrigatório.
Devem ser definidas políticas que garantam a segurança dos dados pessoais, em alinhamento com a estratégia superiormente definida para a segurança do tratamento de dados pessoais.	As políticas que garantam a segurança do tratamento de dados pessoais devem abranger: A priorização e classificação dos dados de acordo com os critérios de sensibilidade e criticidade predefinidos; A criação; A modificação; A transmissão; A recolha (independentemente do respetivo meio ou processo); A destruição; O armazenamento (incluindo a retenção); A pesquisa de dados.	Obrigatório.
	Deve-se garantir o conhecimento, a todo o tempo, dos ativos de informação relativamente a dados pessoais, de modo a permitir identificar inequivocamente o estado da informação em todo o seu ciclo de vida.	Obrigatório.

111231519

FINANÇAS E AMBIENTE

Portaria n.º 87/2018

de 28 de março

O Decreto-Lei n.º 121/2017, de 20 de setembro, define as medidas necessárias ao cumprimento, no território nacional, da Convenção de Washington, sobre o Comércio Internacional das Espécies da Fauna e da Flora Selvagens Ameaçadas de Extinção (CITES) e dos regulamentos comunitários sobre a matéria.

Nesse âmbito, o artigo 38.º do citado diploma legal prevê o pagamento de taxas pela emissão das licenças, certificados e declarações de não inclusão, pela realização de peritagens ou de atos de inscrição ou atualização no registo nacional CITES ou no registo para a detenção de espécimes vivos de espécies previstas na Portaria n.º 86/2018, de 27 de março, remetendo para portaria aprovada pelos membros do Governo responsáveis pelas áreas das finanças e da conservação da natureza o montante das taxas a cobrar pela realização destes atos.

Por outro lado, o artigo 38.º do Decreto-Lei n.º 142/2008, de 24 de julho, prevê a cobrança de taxas pela realização de outros atos de registo e licenciamento da competência do Instituto da Conservação da Natureza e das Florestas, I. P. (ICNF), nomeadamente os relacionados com os detentores de espécimes de espécies listadas nos anexos da Convenção de Berna Relativa à Conservação da Vida Selvagem e dos Habitats Naturais da Europa, aprovada para ratificação pelo Decreto n.º 95/81, de 23 de julho, e regulamentada pelo Decreto-Lei n.º 316/89, de 22 de setembro, com a redação conferida pelo Decreto-Lei n.º 196/90, de 18 de junho, e das espécies abrangidas pela Diretiva n.º 79/409/CEE, do Conselho, de 2 de abril (Diretiva Aves), e Diretiva n.º 92/43/CEE, do Conselho, de 21 de maio (Diretiva Habitats), transpostas para o ordenamento jurídico português pelo Decreto-Lei n.º 140/99, de 24 de abril, alterado e republicado pelo Decreto-Lei n.º 48/2005, de 24 de fevereiro, cujo registo tem vindo a ser regulamentado pela Portaria n.º 7/2010, de 5 de janeiro.

A presente portaria vem, assim, estabelecer o montante das taxas devidas pelos serviços prestados pelo ICNF na qualidade tanto de autoridade administrativa principal