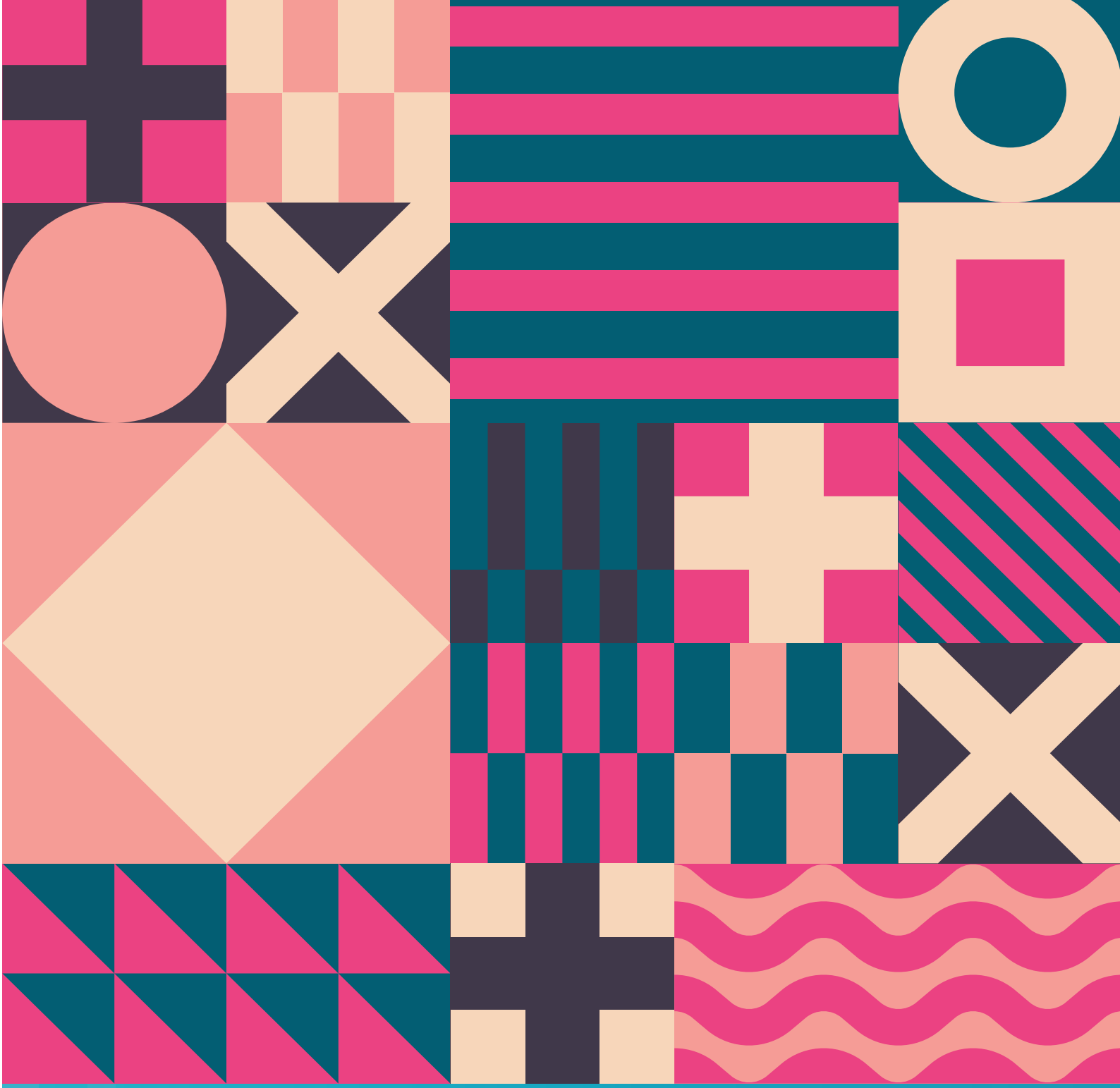

Manual de Boas Práticas Relativamente à Aplicação do Regulamento Geral de Proteção de Dados

ISTEC INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS DE LISBOA

SIGQ_RGPD_MBP_R1_0523

Índice

Introdução

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (doravante designado como RGPD), entrou em vigor em 25 de maio de 2018, enfatizando a proteção das pessoas singulares relativamente ao tratamento de dados pessoais como um direito fundamental.

O RGPD, no Art. 1º(objeto e objetivos), ponto 1, "... estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.", bem como no ponto 2, "o presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.".

O ITA - Instituto de Tecnologias Avançadas para a Formação, Lda, enquanto entidade instituidora do ISTEC Lisboa - Instituto Superior de Tecnologias Avançadas de Lisboa, está comprometido em garantir a privacidade dos dados pessoais rececionados e armazenados nas suas bases de dados.

Nesta conformidade, a Política de Privacidade do ISTEC Lisboa, estabelece que a informação de natureza pessoal é tratada e protegida com toda a diligência e cuidado que o tratamento de dados exige, e de acordo com o Regulamento (UE) 2016/679, RGPD.

O ISTEC Lisboa está fortemente empenhado na proteção dos dados pessoais e no respeito pelo exercício do direito à privacidade dos seus utilizadores. Para ajudar toda a comunidade académica e os seus stakeholders na aplicação de boas práticas relativamente à aplicação da Política de Privacidade do ISTEC Lisboa e do RGPD, criou-se o presente manual que define medidas e práticas concretas que permitem salvaguardar os dados pessoais dos titulares de dados.

Este manual de boas práticas relativamente à aplicação do regulamento geral de proteção de dados foi desenvolvido com o objetivo de fornecer orientações claras e práticas para proteger a segurança e a privacidade dos dados pessoais no nosso ambiente digital cada vez mais conectado. À medida que avançamos na era da transição digital, é essencial adotar medidas eficazes para proteger os nossos sistemas, informações pessoais e a confidencialidade dos dados.

Áreas de utilização de dados pessoais

No ensino superior, a utilização de dados pessoais desempenha um papel fundamental em diversas áreas, contribuindo para a melhoria da qualidade do ensino, o avanço da investigação científica e a personalização da experiência aos estudantes.
A recolha e o processamento de dados pessoais no ISTEC Lisboa ocorrem de forma ética, transparente e em conformidade com o Regulamento Geral de Proteção de Dados (2016/679) e de acordo com a Política de Privacidade do ISTEC Lisboa.

As áreas onde são recolhidos, processados e utilizados os dados, são:

1. Gestão Académica

Para que lhe possamos proporcionar as condições necessárias para construir um percurso académico e assegurar o cumprimento com todas as obrigações legais a que estamos sujeitos, os seus dados pessoais serão tratados, nomeadamente, para as seguintes finalidades:

a. Gestão de matrícula e inscrições;
b. Manutenção e atualização do processo individual de estudante;
c. Concessão de estatutos especiais de frequência;
d. Gestão de programas de mobilidade de caráter nacional e/ou internacional;
e. Reconhecimento de equivalências e de documentos conferentes de graus e demais títulos académicos;
f. Emissão de certificados e diplomas;
g. Manutenção do seguro escolar e participação de sinistros;
h. Gestão admirativa das bolsas da DGES;
i. Gestão de assiduidade, classificações e outras informações académicas;
j. Gestão de outros apoios sociais.

2. Investigação Científica

No âmbito da missão a que se encontra adstrita enquanto instituição de ensino superior, o ISTEC Lisboa assume como um dos seus principais objetivos a promoção da investigação científica, tendo em vista não só a produção e difusão de conhecimento, como também a própria valorização da atividade dos seus docentes, investigadores e estudantes.

Neste contexto, poder-lhe-á ser solicitada a colaboração em projetos promovidos por membros da comunidade académica do ISTEC Lisboa no âmbito dos respetivos ciclos de estudos ou atividades de investigação. Os dados concretos a recolher e a finalidade da sua recolha dependerão do projeto de investigação em causa, tal como o formato do próprio estudo. Em qualquer dos casos, a sua participação será sempre voluntária e os seus dados pessoais apenas serão tratados mediante o seu consentimento, no estrito cumprimento dos padrões éticos reconhecidos pela comunidade científica e de acordo com o Código de Ética e Conduta do ISTEC Lisboa.

3.Videovigilância

Para zelar pela sua segurança e de todos aqueles que connosco se relacionam, bem como dos bens que se situam no nosso perímetro (Campus Académico do Lumiar, sejam estes do ISTEC Lisboa ou de terceiros, o ISTEC Lisboa dispõe de Sistemas de Videovigilância em vários pontos das suas instalações.

Todas as câmaras encontram-se instaladas em estreita consonância com os requisitos legalmente prescritos.

4. Prestação de Serviços à Comunidade

Através do ISTEC Lisboa e da sua Unidade de Investigação em Computação Avançada (UICA), ou de estruturas especialmente montadas para o efeito, o ISTEC Lisboa coloca os seus saberes ao dispor da comunidade, na forma de serviços prestados nos mais variados campos de conhecimento, com especial destaque na área das tecnologias de informação. Nesse sentido, poderá nomeadamente aceder aos laboratórios, salas de aulas práticas, salas de aulas teóricas, auditórios, entre outros.

Os dados pessoais que fornecer neste contexto serão única e exclusivamente utilizados para a prestação dos serviços que requisitar, bem como, atenta a missão do Instituto, garantir a formação dos seus estudantes e promover a investigação científica.

5. Antigos Estudantes

Nesse sentido, para além de outras comunicações que possa eventualmente subscrever, ser-lhe-ão enviadas, via correio eletrónico, comunicações relacionadas com:

a. Notícias do ISTEC Lisboa;
b. Iniciativas de sucesso profissional de alumni (publicações, livros, blogues, cargos, programas televisivos, etc.);
c. Inquéritos sobre empregabilidade;
d. Divulgação de oportunidades profissionais;
e. Oferta de formação contínua;
f. Eventos especificamente dirigidos ao público alumni.

Poderá a qualquer momento cancelar, sem necessidade de apresentar justificação, o recebimento de tais comunicações.

6. Eventos e outras iniciativas

No âmbito de iniciativas promovidas pelo ISTEC Lisboa (Workshops, Seminários, Conferências, Feiras de Emprego, etc.), poderão ser solicitados alguns dos seus dados pessoais para efeitos de gestão da sua inscrição e credenciação, bem como de faturação (em caso de eventos pagos).

Adicionalmente, poderá ainda haver lugar à captação de fotografias e/ou vídeos para efeitos de divulgação e promoção em canais de comunicação internos e externos.

7. Comunicações Institucionais

Por forma a divulgar as atividades desenvolvidas pelo ISTEC Lisboa e informá-lo sobre a vida do Instituto e dos diferentes organismos pertencentes à comunidade académica, poderá receber diferentes tipos de comunicações, tais como:

a. Newsletters;
b. Divulgação da oferta formativa do Instituto;
c. Divulgação de oportunidades profissionais;
d. Divulgação de informações do Conselho Técnico-Científico, Conselho Pedagógico e Provedor do Estudante;
e. Divulgação de iniciativas da Associação de Estudantes do Instituto Superior de Tecnologias Avançadas de Lisboa (AEISTEC);
f. Pedidos de colaboração em atividades de investigação científica.

8. Cartão Estudante

Resultado de uma parceria com a Caixa Geral de Depósitos, o Cartão Estudante do ISTEC Lisboa é o seu documento de identificação como membro da comunidade académica, garantindo-lhe o acesso a um conjunto alargado de serviços do Instituto e de instituições parceiras. Para mais informações sobre a Política de Privacidade e Proteção de Dados Pessoais da Caixa Geral de Depósitos, consultar aqui:
https://www.cgd.pt/Ajuda/Pages/Politica-Privacidade-Protecao-Dados-Pessoais.aspx

9. Infraestruturas Tecnológicas

Caso utilize as infraestruturas tecnológicas do ISTEC Lisboa, incluindo redes wi-fi, alguns dos seus dados pessoais serão automaticamente recolhidos e analisados, por forma a monitorizar a segurança dessas infraestruturas e prevenir utilizações abusivas das mesmas.

10. Cookies

Os portais do ISTEC Lisboa utilizam cookies para assegurar a melhor experiência de utilização possível sempre que nos visita. Os cookies são pequenos ficheiros eletrónicos armazenados no seu dispositivo, que permitem às plataformas distinguir cada visitante e manter as suas preferências ao longo da respetiva sessão. Os cookies utilizados pelo ISTEC Lisboa respeitam o anonimato e não serão usados para recolher informação de caráter pessoal.

Nos portais do ISTEC Lisboa é utilizado o serviço Google Analytics, cujas informações armazenadas nos cookies são mantidas pela Google para fins estatísticos e de análise de pesquisas. Para mais informações sobre os tipos de cookies utilizados pela Google poderá consultar as políticas de privacidade aqui: https://policies.google.com/privacy

11. Gestão Administrativa

Para assegurar o regular funcionamento do ISTEC Lisboa, poderão ser tratados alguns dos seus dados pessoais para:

a. Apoio à tomada de decisão e à melhoria contínua dos processos internos;
b. Emissão do cartão de estudante;
c. Controlo e gestão do acesso e utilização de serviços do ISTEC Lisboa, tais como biblioteca, infraestruturas desportivas e tecnológicas, entre outros;
d. Processamento de pagamentos;
e. Apreciação de reclamações, requerimentos, recursos e procedimentos similares;
f. Gestão de procedimentos eleitorais;
g. Realização de auditorias e procedimentos de certificação e acreditação;
h. Preenchimento, para comunicação à Direção-Geral de Estatística da Educação e Ciência, dos inquéritos RAIDES, RENATES, entre outros;
i. Cumprimento com outras obrigações jurídicas, incluindo a cooperação com as autoridades competentes;
j. Comunicações em caso de eventuais emergências.

Boas Práticas no Tratamento de Dados por Área

O tratamento responsável e ético dos dados pessoais no ISTEC Lisboa é um elemento essencial para garantir a confidencialidade, integridade e privacidade das informações dos estudantes, docentes e demais membros da comunidade académica.

Para cada área funcional, existe um conjunto de boas práticas que devem ser observadas, são elas:

1. Serviços Académicos

1.1. Guardar dados para futuro contacto (ex.: divulgação de oferta formativa)

Caso exista a necessidade de ficar com os dados para um futuro contacto, deve-se solicitar o consentimento do titular dos dados para essa finalidade.

Caso este indique que não pretende que se guarde os dados pessoais, deve-se apagar os dados fornecidos (consequência da recusa de consentimento), podendo-se enviar um email para esse efeito.

1.2. Recolha de documentos pessoais

Relativamente à recolha de dados como a reprodução do cartão de cidadão em fotocópia ou qualquer outro documento de identificação (cartão com o NIF + Bilhete de Identidade + Cartão da Segurança Social) sem consentimento do titular dos dados, não deve ser aceite pelos Serviços Académicos.

Deve-se usar o carimbo com a indicação "Autorizo a cópia do documento" com a respetiva data e assinatura do titular dos dados.

Por outro lado, caso o titular dos dados não pretenda fornecer tem direto à oposição, e nesse caso, deverá ser colocado um carimbo que os dados estão conforme documento original, devidamente exibidos. Colocar a assinatura do título dos dados e do colaborador que tratou deste processo.

1.3. Receção de dados pessoais na celebração da matrícula

O aluno toma conhecimento das condições de frequência no curso ou do ciclo de estudos em que se matrícula, assumindo inteira responsabilidade, nos termos da lei, pela exatidão dos dados constantes nessa ficha.

Informações gerais:

a. As pessoas que se apresentarem como familiares ou tutores do(a) aluno(a) apenas podem obter informação na presença do(a) aluno(a), ou caso este(a) não esteja presente, apenas com procuração assinada pelo(a) aluno(a) a conferir poderes para o efeito;

b. Os dados dos alunos, arquivados digitalmente, devem estar organizados por pastas de acesso reservado e condicionado ao responsável do serviço, com password de acesso e na sua área reservada. As pastas não devem estar armazenadas no ambiente de trabalho;

c. Os processos físicos dos alunos, não devem ser consultados à frente de terceiros, devendo garantir-se a devida confidencialidade;

d. O contacto com o Serviço de Estrangeiros e Fronteiras (SEF) deverá ser precedido de autorização escrita do titular dos dados para que os dados fornecidos àquele Serviço (nome, data de nascimento, nacionalidade) para agendamento de extensão do visto, esteja coberto pelas regras constantes do RGPD;

e. Quando os docentes se encontrem no espaço dos Serviços Académicos, o trabalho em curso deve ficar devidamente ocultado ao docente, exceto se o docente solicitar informações sobre um determinado aluno, caso em que a informação deverá ser disponibilizada, mas de forma reservada e cingir-se ao estritamente necessário;

f. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

g. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade.

2. Serviços Financeiros e Tesouraria

2.1. Recolha de dados pessoais dos colaboradores

A recolha de dados pessoais do colaborador, como morada, o telemóvel, o endereço eletrónico, o nome do cônjuge e seus dependentes, datas de nascimento dos mesmos, entre outros, deve ser feita numa ficha própria para o efeito e arquivada em suporte de papel em armário fechado à chave e arquivado digitalmente, com proteção de password em pasta codificada.

2.2. Recolha de documentos pessoais

Relativamente à recolha de dados como a reprodução do cartão de cidadão em fotocópia ou qualquer outro documento de identificação (cartão com o NIF + Bilhete de Identidade + Cartão da Segurança Social) sem consentimento do titular dos dados, não deve ser aceite pelos Serviços.

Deve-se usar o carimbo com a indicação "Cópia autorizada pelo próprio" em todos os documentos cujo exista reprodução.

Por outro lado, caso o titular dos dados não pretenda fornecer tem direto a posição, e nesse caso, deverá ser colocado um carimbo que os dados "está conforme documento original", estes documentos devem ser exibidos. Colocar a assinatura do título dos dados e do colaborador que tratou deste processo.

Informações gerais:

a. Os dados dos colaboradores (docentes e não docentes), arquivados digitalmente, devem estar organizados por pastas de acesso reservado e condicionado ao responsável do serviço, com password de acesso e na sua área reservada. As pastas não devem estar armazenadas no ambiente de trabalho;

b. Os dados dos colaboradores arquivados digitalmente, devem estar organizados por pastas de acesso reservado e condicionado ao responsável do serviço, com password de acesso e na sua área reservada. As pastas não devem estar armazenadas no ambiente de trabalho;

c. Os processos físicos dos colaboradores, não devem ser consultados à frente de terceiros, devendo garantir-se a devida confidencialidade;

d. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

e. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade.

3. Gabinete de Comunicação e Relações Públicas

O direito à imagem é um direito de personalidade, constitucionalmente consagrado e protegido (n.º1 do artigo 26.º da CRP).

A captação e/ou divulgação de imagem devem ser precedidas de consentimento pelo titular, que deve conhecer as finalidades do uso da sua imagem, podendo opor-se ao seu tratamento, arquivo, divulgação, a todo o tempo.

Contudo, o número 2 do artigo 79.º do Código Civil refere "Não é necessário o consentimento da pessoa retratada quando assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente."

Apenas nestes casos pode não ser necessário o consentimento, porém, atenta a publicação do RGPD e as preocupações expostas com esta temática, designadamente por causa das redes sociais, o pedido de consentimento deve ser sempre pedido e arquivado.

Este pedido deve ser feito a estudantes, docentes, não docentes, pessoal externo à organização (ex.: convidados de palestras).

Informações gerais:

a. O tratamento de dados pessoais que envolvam a captação e recolha de imagem ou vídeo necessitam do consentimento prévio dos envolvidos. O consentimento é expresso, inequívoco, contendo as finalidades, designadamente onde e como vai ser publicada a imagem ou vídeo, a identificação do evento, o prazo de publicação, o direito de oposição;

b. As fotografias e vídeos devem ser destruídos após o prazo definido para a sua publicação e tratamento;

c. A publicidade do ISTEC Lisboa que contenha a imagem ou vídeo de pessoas individuais deve ter associado o consentimento expresso dos titulares dos dados. Este tipo de publicidade deve ter um período mais reduzido de vigência. Quanto maior a exposição dos intervenientes e titulares dos dados, menor deve ser a duração da campanha publicitária;

d. As fotografias captadas em eventos organizados pelo ISTEC Lisboa, ou organizados e realizados no Campus Académicos do Lumiar, não devem identificar pessoas individuais, sem o prévio consentimento das mesmas. Caso este consentimento não seja passível de obtenção, as fotografias devem ser desfocadas ao ponto de a imagem não permitir a identificação da pessoa individual ou focar-se, em alternativa, as pessoas de costas;

e. A divulgação da oferta formativa do ISTEC Lisboa nas escolas secundárias e em escolas profissionais, representa, especial sensibilidade se tivermos como público pessoas menores de idade. Neste caso, é necessária a autorização dos Encarregados de Educação para a recolha dos dados pessoais, sem a qual não pode ser aceite, ainda que livremente disponibilizados pelo menor, quaisquer dados ou informação pessoal;

f. Os cartões-de-visita pedidos por docentes e investigadores e pessoal técnico, administrativo e de gestão, com autorização para o efeito, devem, caso manifeste vontade na publicação do seu contacto móvel privado e pessoal, ser precedido de consentimento expresso;

g. As publicações nas redes sociais onde são utilizadas imagens, na partilha de informações ou campanhas publicitárias, não devem identificar pessoas individuais, sem o prévio consentimento das mesmas. Caso este consentimento não seja passível de obtenção, as fotografias devem ser desfocadas ao ponto de a imagem não permitir a identificação da pessoa individual ou focar-se, em alternativa, as pessoas de costas;

h. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

i. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade.

4. Gabinete de Apoio ao Estudante e à Empregabilidade

Os e-mails rececionados, provenientes de empresas parceiras, bem como informações enviadas pelos estudantes, devem ser visualizados apenas pelas pessoas que integram o Gabinete de Apoio ao Estudante e à Empregabilidade.

Informações gerais:

a. No preenchimento do inquérito de interesse sobre as preferências na realização de estágios curriculares, deve-se obter o consentimento explícito e informado dos estudantes, antes da recolha, processamento ou compartilha de dados pessoais. Deve ser garantido que os estudantes estão cientes de como os seus dados pessoais serão utilizados.

b. Devem ser recolhidos apenas os dados pessoais estritamente necessários para cumprir as finalidades específicas do gabinete, evitando a recolha excessiva de informações e garantir que a retenção dos dados seja limitada ao período necessário;

c. Fornecer aos estudantes informações claras e transparentes sobre como os seus dados pessoais são tratados, não só pelo ISTEC Lisboa, mas como pelas empresas parceiras aquando da realização dos seus estágios curriculares.

d. Garantir que os estudantes possam aceder aos seus próprios dados pessoais e, se necessário, corrigi-los ou atualizá-los, estabelecendo procedimentos para que os estudantes possam exercer o seu direito de acesso e retificação de forma fácil e eficiente;

e. Limitar a partilha de dados pessoais com terceiras apenas às finalidades autorizadas e com base em acordo de confidencialidade e proteção de dados adequados;

f. Nos protocolos de Formação de Contexto de Trabalho realizados no cumprimento dos estágios curriculares de todos os cursos do ISTEC Lisboa, deve-se assegurar que são incluídas cláusulas que garantam de forma expressa e inequívoca que os estudantes obrigam-se a não divulgar ou transmitir, direta ou indiretamente, a quaisquer terceiros, dados ou factos de natureza confidencial relativos à empresa formadora, respetiva organização, seus negócios, produtos, clientes, estratégias, procedimentos, equipamentos, processos de fabrico ou atividade por esta desenvolvida, proibição esta que vigora quer durante a vigência do estágio curricular, quer após a sua extinção;

g. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

h. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade.

5. Gabinete de Projetos Educativos e Internacionalização

Os e-mails rececionados, provenientes de Instituições de Ensino Superior Estrangeiras devem ser visualizados apenas pelas pessoas que integram o Gabinete de Projetos Educativos e Internacionalização.

Informações gerais:

a. Os dados introduzidos no Sistema da Agência Nacional no âmbito do Programa Erasmus +, deverá ser efetuado apenas por uma pessoa. A obtenção dessa informação por correio eletrónico deve observar as medidas anteriormente referidas. Importa tratar os dados por forma a garantir a confidencialidade dos mesmos;

b. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

c. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade.

6. Gabinete da Qualidade

Os e-mails rececionados, provenientes de Instituições externas e de toda a comunidade académica do ISTEC Lisboa, devem ser visualizados apenas pelas pessoas que integram o Gabinete do Sistema Interno de Garantia de Qualidade

Informações gerais:

a. Os dados recolhidos através de inquéritos devem ser anonimizados (se aplicável) antes da divulgação;

b. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

c. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade.

7. Gabinete de Informática e Sistemas

O Gabinete de Informática e Sistemas, por inerência de funções, é a unidade de apoio técnico do ISTEC Lisboa, exercendo a sua função no domínio do planeamento, implementação, gestão, suporte e promoção da utilização dos serviços de comunicações e informática, e dos sistemas de informação.

7.1. Acesso ao computador e à rede informática

O acesso a dados pessoais ou classificados como sensíveis, diretamente de computadores ou através da rede informática interna do ISTEC Lisboa, deve ser segmentado com níveis de acesso diferentes, tendo o colaborador apenas acesso a áreas que lhe compete, consoante as suas funções e a necessidade de acesso a determinados dados pessoais e/ou sensíveis, e com segurança realizada através da definição de passwords fornecidas aos colaborados do ISTEC Lisboa.

7.2. Acesso a softwares e contas de e-mails institucionais

O acesso a dados pessoais ou a dados classificados como sensíveis, diretamente de computador, ou através da rede informática interna do ISTEC Lisboa ou até dos que se encontram "alojados" em softwares de faturação, gestão de salários, etc. e os dados que possam eventualmente se encontrar em caixas de e-mail do ISTEC Lisboa, deve ser segmentado com níveis de acesso diferentes, tendo o colaborador apenas acesso a áreas que lhe compete, consoante as suas funções e a necessidade de acesso a determinados dados pessoais e/ou sensíveis, e com segurança realizada através da definição de passwords fornecidas aos colaborados do ISTEC Lisboa.

7.3. Cópias de segurança

Em colaboração com os diferentes serviços, o Gabinete de Informática e Sistemas, e de acordo com o que o RGPG e a Política de Privacidade do ISTEC Lisboa obrigam, devem criar mecanismos regulares e encriptados das referidas cópias e ficheiros cujo acesso livre apenas possa ser dado ao responsável pela proteção de dados da instituição.

Informações gerais:

a. Colaborar com outros serviços para a realização de avaliações de impacto de proteção de dados sempre que necessário, especialmente em serviços e projetos que envolvam o processamento de dados pessoais sensíveis ou de grande escala, identificando e mitigando riscos relacionados à privacidade e segurança de dados;

b. Implementar medidas e técnicas adequadas para garantir a segurança dos dados pessoais sobre a responsabilidade do gabinete de informática e sistemas, incluindo a implementação de controlos de acesso, criptografia de dados, monitoração de segurança, backups regulares e planos de resposta a incidentes de segurança;

c. Devem ser estabelecidas políticas e procedimentos para gerir de forma adequada os acessos aos sistemas e dados pessoais, garantindo que apenas as pessoas autorizadas tenham acesso aos dados necessários para o cumprimento das suas funções;

d. Incorporar princípios de privacidade desde o início do desenvolvimento e implementação de sistemas e softwares. Considerar medidas técnicas que garantam a proteção de dados pessoais, como a minimização de dados, o anonimato, a pseudonimização e a implementação de configurações de privacidade por padrão;

e. Estabelecer políticas claras de retenção e eliminação de dados pessoais, garantindo que os dados sejam mantidos apenas pelo tempo necessário e que sejam adequadamente destruídos quando não forem mais necessários, de acordo com os requisitos legais e regulamentares;

f. Deve ser implementado e aplicada a "política de mesa limpa e utilização de equipamento", ou seja, não devem estar expostos dados pessoais e com acesso condicionado no espaço de trabalho;

g. As assinaturas dos endereços de correio eletrónico devem conter uma mensagem de confidencialidade;

Boas Práticas de Segurança e Privacidade

A segurança e a privacidade são preocupações críticas em todos as áreas de atuação do ISTEC Lisboa. Ao seguir as práticas delineadas neste manual, podemos mitigar os riscos de violações de segurança e de privacidade e cumprir com as obrigações legais relacionadas com a proteção de dados, promovendo, igualmente uma abordagem em camadas para a segurança e a privacidade, abrangendo tanto as medidas técnicas quanto as práticas comportamentais. Inclui recomendações sobre a adoção de sistemas de autenticação robustos, a implementação de firewalls e criptografia de dados, a realização de backups regulares, a sensibilização dos funcionários sobre phishing e outras ameaças, além de diretrizes para o compartilhamento seguro de informações e o cumprimento das políticas internas de segurança.

1. Privacidade e Proteção de Dados Pessoais

O Regulamento Geral de Proteção de Dados foi publicado no Jornal Oficial da União Europeia e é aplicável a partir do dia 25 de maio de 2018.

Relativamente ao novo regulamento, é importante saber que:

a. Dados pessoais são todas as informações relativas a uma pessoa identificada ou identificável (nome, morada, património, vencimento, datas, números de cartões, nº de telefone, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, curriculum vitae, etc);

b. Existe um Encarregado de Proteção de Dados (EPD) no ISTEC Lisboa, que poderá ser contactado através de endereço de email protecao.dados@istec.pt;

c. Ao enviar dados pessoais para outros, estes deverão ser encriptados ou protegidos com palavra-passe (a palavra-passe não deverá ser enviada via correio eletrónico);

d. Deverá existir cuidado redobrado no tratamento de documentos com informações críticas como é o caso de dados médicos ou de menores;

e. Antes de remeter informação via correio eletrónico com caráter de divulgação, tal como informação sobre ações de formação, oferta formativa ou outra de natureza afim, certifique-se que o destinatário da mensagem deu o seu consentimento para o envio desse tipo de informação. Caso não possua seu consentimento, procure obtê-lo, por correio eletrónico, antes do envio da informação;

f. Ao destruir ou eliminar dados pessoais, estes devem ser apagados/destruídos de forma definitiva, garantindo assim que não serão recuperados por terceiros;

g. Quando existir violação de dados pessoais e considere-se por violação de dados pessoais uma violação de segurança que provoque, seja de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou acesso não autorizado, a dados pessoais deverá reportar de imediato o incidente de segurança de através de protecao. dados@istec.pt;

h. O EPD tem a responsabilidade e obrigação de comunicar as autoridades todas as fugas ou perdas de dados pessoais ocorridos na organização, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

2. Correio Eletrónico

O correio eletrónico é o serviço de comunicação mais usado nas organizações, nesse sentido é também uma fonte de riscos e um dos meios mais usados para a difusão de programas maliciosos. Cada utilizador é responsável pela utilização e atividades associadas à sua conta de correio eletrónico. O seu uso deve ser efetuado de maneira apropriada, não atentando contra a imagem ou funcionamento do ISTEC Lisboa. É, por isso, proibida a utilização do serviço de correio eletrónico para o envio de informação ou conteúdos ofensivos ou inadequados. Na mesma linha, é também proibido o uso do correio eletrónico do ISTEC Lisboa para o tratamento de assuntos de cariz pessoal.

2.1. Reencaminhamento de conta de correio eletrónico

Não é aconselhável o reencaminhamento de correio eletrónico de contas internas para contas externas. O reencaminhamento de mensagens entre caixas de correio internas também é desaconselhado, e só deve acontecer com autorização dos donos das contas de correio eletrónico ou em casos especiais (exemplo: doença, férias, entre outros).

2.2. Verificar destinatários

Quando enviar mensagens, é indispensável garantir que os destinatários que incluiu estão corretos, ou seja, se são os destinatários que devem receber e ter acesso à informação que está a enviar. Se for necessário, utilize convenientemente as opções "Cópia oculta" e "Responder a todos".

2.3. Anexos a mensagens

O correio eletrónico é um meio popular de propagação de software malicioso (malware). É importante que esteja ciente deste facto quando receber mensagens de correio que contenham anexos ou hiperligações para efetuar downloads de sites externos. Como os antivírus não são infalíveis, a melhor defesa é a prudência, sendo aconselháveis as seguintes ações:

a. Não abrir anexos de origem desconhecida;
b. Não abrir anexos de endereços conhecidos que não esperava receber;
c. Nunca abrir anexos que tenham extensões executáveis (.exe, .bat, .com, .dll);
d. Não abrir anexos que tenham mais de uma extensão;
e. Em caso de dúvida, consultar o Gabinete de Informática e Sistemas para pedir esclarecimentos.

2.4. Informações críticas e pessoais

Informações críticas, confidenciais ou outro tipo de informações relativas a dados pessoais/privados, só devem ser enviados via correio eletrónico em formatos encriptados. As chaves/palavras-passe usadas nestes processos devem ser enviadas através de outro meio de comunicação.

2.5. Aviso/Disclaimer

Quando envia informação sensível (exemplo: possuindo dados pessoais, privados, com classificação secreta ou confidencial), a mensagem de correio eletrónico deverá ser acompanhada de um aviso/disclaimer informando que a informação enviada se destina exclusivamente ao(s) destinatário(s), pelo que a sua distribuição é proibida.
Exemplo "Esta mensagem contém informação classificada de confidencial ou privilegiada. Em caso de a ter recebido inadvertidamente, por favor contacte o remetente por correio eletrónico e apague a mensagem assim como todos os seus dados."

3. Política de Mesa Limpa e Utilização de Equipamento

Todos os membros da comunidade académica do ISTEC Lisboa, deverão ter em conta a política de mesa limpa, de modo a garantir que informação privada, secreta ou confidencial não é divulgada.

Deste modo as seguintes ações deverão ser tomadas em conta:

a. A mesa de trabalho deverá ser limpa de qualquer documento ou suporte de informação, que contenha dados pessoais ou informações secretas e/ou confidenciais, quando deixado sem supervisão por um longo período de tempo, assim como no final do dia de trabalho;

b. Toda a informação com dados pessoais, privados, secretos e confidenciais deverá ser retirada da mesa depois de utilizada e armazenada num local seguro e com controlo de acessos;

c. Todos os documentos e suportes físicos de informação devem ser guardados em gavetas adequadas com fechaduras e/ou outra forma segura de mobiliário, quando não estiverem a ser utilizados, especialmente fora dos horários de trabalho;

d. Os computadores e dispositivos móveis deverão ser bloqueados sempre que o utilizador se ausentar, e desligados no final do dia de trabalho;

e. Todas as impressões com informação pessoal, privada, secreta ou confidencial, utilizada ou processada por equipamentos de suporte, por exemplo impressoras, fotocopiadoras e/ou digitalizadores, devem ser retiradas dos mesmos imediatamente após o seu processamento terminar;

f. Nenhuma informação de acesso reservado pode ser retirada das instalações sem autorização;

g. Fora das instalações do ISTEC Lisboa, qualquer elemento da comunidade académica é responsável pela salvaguarda do equipamento e da informação a ele confiadas.