Política de Privacidade e Proteção de Dados

Data Privacy and Protection Policy

Autor/Author:
Encarregado de Proteção de Dados (DJU)/Data Protection Officer

Aprovado por/Approved by:
CEO & COO
Procuradores/Power of Atorney

Em vigor a partir de/Effective from:
21/11/2023

Sumário/Overview:

A presente Política visa reforçar o compromisso da T.S.T. – Transportes Sul do Tejo, S.A. (TST), no cumprimento de toda a legislação e regulamentações aplicáveis à sua atividade, assegurando os mais elevados padrões de conduta, honestidade e integridade.

O Regulamento Geral de Proteção de Dados (RGPD), em vigor desde 25 de maio de 2018, deve ser rigorosamente cumprido pelos Trabalhadores e por todos os que trabalham para e em nome da Empresa, e no âmbito da presente Política toda e qualquer violação da Política e da Legislação Local ou Europeia, deve ser denunciada de imediato, fomentando uma cultura de abertura, transparência e responsabilização.

This policy aims to reinforce the commitment of T.S.T. – Transportes Sul do Tejo, S.A. (TST), with compliance with all legislation and regulations that apply to its business activity, ensuring the highest standards of conduct, honesty, and integrity.

The Data Protection Regulation, in place since may 25, 2018, must be strictly complied with by Employees and everyone who works for and on behalf of the Company, and in the scope of this Policy any and all violations of this Policy and Local or European Legislation, must be reported immediately, fostering a culture of openness, transparency and accountability.

Índice/Index

1. Aplicação e âmbito da Política /*Policy purpose and scope*

A TST tem como compromisso assegurar a privacidade e proteção de dados pessoais de todos os que com ela colaboram. Esta Política destina-se a toda a Empresa, a todos os Trabalhadores, quer trabalhem a tempo inteiro, a tempo parcial, com contrato ou como temporários. Aplica-se a candidatos, ex-trabalhadores, mas também aos prestadores de serviços, fornecedores (ou quaisquer pessoas sob a supervisão destes), os titulares de participações sociais ou membros de órgãos estatutários, ou estagiários (independentemente de serem ou não remunerados).

Esta Política está em conformidade com o **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho Europeu, de 27 de abril de 2016,** e com a **Lei nº58/2019 de 8 de agosto de 2019**, a qual estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na União Europeia.

TST is committed to ensure the privacy and protection of personal data of everyone who works with TST. This Policy is intended for the entire Company, for all Workers, whether they work full-time, part-time, on a contract or as temporary workers. It applies to candidates, former workers, but also to service providers, suppliers (or any people under their supervision), holders of social shares or members of statutory bodies, or interns (regardless of whether they are paid or not).

This Policy is in accordance with **Regulation (EU) 2016/679 of the European Parliament and the European Council, of April 27, 2016,** and with **Law nº58/2019 of August 8, 2019,** which establishes the rules relating to the processing, by a person, company, or organization, of personal data relating to people in the European Union.

2. Responsabilidade do Tratamento de Dados Pessoais /*Personal Data Treatment Responsibility*

Entidade responsável pela recolha e tratamento dos dados pessoais:

T.S.T. – Transportes Sul do Tejo, S.A.
Rua Marcos Portugal, Laranjeiro, 2810 – 260 Almada, Portugal
Telefone: +351 210 000 700 | Web: **www.tsuldotejo.pt**

Contudo, no âmbito da sua atividade, poderá recorrer a entidades por si subcontratadas para a prossecução das finalidades aqui indicadas. Neste caso, estas entidades ficam igualmente obrigadas a desenvolver as medidas técnicas e organizativas adequadas a garantir que o tratamento dos dados pessoais satisfará os requisitos legais, designadamente no domínio da segurança e confidencialidade, de forma a assegurar a defesa dos direitos dos titulares dos dados. De realçar que a TST por sua vez é igualmente subcontratada pela Transportes Metropolitanos de Lisboa (TML), para efeito de tratamento de dados sensiveis dos Clientes da Área Metropolitana de Lisboa, os quais são efetuados de acordo com as normas impostas pela entidade.

Entity responsible for collecting and processing personal data:

T.S.T. – Transportes Sul do Tejo, S.A.
Rua Marcos Portugal, Laranjeiro, 2810 – 260 Almada, Portugal
Telephone: +351 210 000 700 | Web: www.tsuldotejo.pt

However, within the scope of its activity, it may use entities subcontracted by it to pursue the purposes indicated here. In this case, these entities are also obliged to develop appropriate technical and organizational measures to ensure that the processing of personal data will meet legal requirements, particularly in the area of security and confidentiality, in order to ensure the defence of the rights of data owners. It should be noted that TST, in turn, is also subcontracted by Transportes Metropolitanos de Lisboa (TML), for the purpose of processing sensitive data from Customers in the Lisbon Metropolitan Area, which is carried out in accordance with the standards imposed by the entity.

3. Finalidade dos Dados Pessoais Recolhidos / *Purpose of Collected Personal Information*

Recolhemos dados pessoais sobre todos os visados pela presente Política, e apenas os indispensáveis à prestação da sua atividade profissional e cumprimento das inerentes obrigações legais.

Os dados pessoais recolhidos não serão transmitidos a terceiros sem o consentimento expresso dos seus titulares, exceto nas situações em que seja indispensável para o cumprimento das finalidades acima referidas, caso em que a TST exigirá a esses terceiros que apliquem as medidas necessárias com o intuito de satisfazer o cumprimento dos requisitos legais.

Para o efeito exclusivo de cumprimento de obrigações legais, a TST poderá permitir o acesso aos dados pessoais dos titulares, quando solicitados por Autoridades Judiciais, de Segurança Pública, Tributárias ou Regulatórias.

We collect personal data about everyone covered by this Policy, and only the essential to rendering their professional activity and fulfilment with inherent legal obligations.

The personal data collected will not be transmitted to third parties without the express consent of their owners, except in situations where it is essential to fulfil the purposes above mentioned, in which case TST will require these third parties to apply the necessary measures to fulfil with compliance and legal requirements.

For the exclusive purpose of complying with legal obligations, TST may allow access to holders' personal data, when requested by Judicial Public Security, Tax or Regulatory Authorities.

4. Atividades de Tratamento de Dados e Prazos de Conservação / *Data processing activities and Retentions period*

O registo das atividades de tratamento de dados é uma obrigação, imposta pelo artigo 30.º do RGPD, para os responsáveis pelo tratamento e para os subcontratantes. Desta forma a TST assegura o registo das atividades de tratamento e respetivos prazos de conservação em linha com o modelo disponibilizado com as obrigações de registo de atividades de tratamento da Comissão Nacional de Proteção de Dados (**CNPD**).

Os dados pessoais são conservados apenas pelo período necessário para cumprimento da finalidade que motivou o seu tratamento, sem prejuízo do cumprimento dos prazos legalmente definidos.

The data processing activities registry is an obligation, imposed by article 30º from GDPR, for the processing owners and subcontractors. In this way TST assures the data processing activities registry and respective retention periods in line with the model made available with the registration obligations of processing activities from Comissão Nacional de Proteção de Dados (**CNPD**).

The personal data will be only stored for the period necessary to fulfil the purpose that originated its processing, without prejudice of complying with of the legally defined deadlines.

5. Direitos dos Titulares de Dados Pessoais / *Owner of Personal Data Rights*

Os titulares dos dados pessoais, têm o direito de acesso, atualização, retificação, eliminação, portabilidade e apagamento dos seus dados pessoais. Podem ainda determinar limites ou opor-se ao seu tratamento, com exceção no que respeita aos dados pessoais indispensáveis à prestação da sua atividade profissional e/ou ao cumprimento de obrigações legais. Os consentimentos que venham a ser dados pelos titulares podem também ser retirados a qualquer momento.

Contudo, a sua retirada não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Os titulares têm o direito de serem notificados pela TST caso exista uma violação dos seus dados pessoais e podem, ainda, apresentar reclamação à autoridade de controlo – a CNPD - sem prejuízo de poderem igualmente, reclamar junto do Encarregado da Proteção de Dados da TST.

Owners of personal data have the right to access, update, rectify, delete, portability and erase their personal data. They may also determine limits or even oppose their processing, except for personal data essential to fulfil their professional activity and/or the compliance with legal obligations. Consents that may be given by data owners may also be withdrawn at any time.

However, its withdrawal does not compromise the lawfulness of the processing carried out based on the consent previously given. Owners have the right to be notified by TST if there is a breach of their personal data and may also file a complaint with the supervisory authority - the CNPD - without prejudice of also being able to complain to TST Data Protection Officer.

6. Contacto do Encarregado da Proteção de Dados / *Data Protection Owner contact*

O Encarregado da Proteção de Dados deverá ser contactado através de carta enviada para:

T.S.T. – Transportes Sul do Tejo, S.A.
Rua Marcos Portugal, Laranjeiro, 2810 – 260 Almada, Portugal

Ou através do seguinte endereço de e-mail: gdpr@tst.com.pt

The Data Protection Officer should be addressed by letter sent to:
T.S.T. – Transportes Sul do Tejo, S.A.
Rua Marcos Portugal, Laranjeiro, 2810 – 260 Almada, Portugal

Or through e-mail address: gdpr@tst.com.pt

7. Medidas de Segurança dos Dados Pessoais / *Personal Data Protection Security Measures*

A TST aplica as medidas adequadas de forma a satisfazer os requisitos legais, designadamente no âmbito da segurança e confidencialidade. A TST procura assim assegurar a defesa dos direitos dos titulares dos dados pessoais, por forma a garantir a respetiva proteção dos mesmos dentro das obrigações legais que abrangem a TST.

As referidas medidas serão alvo de revisão e de melhoria contínua, sendo os sistemas informáticos monitorizados constantemente, com intuito de prevenir, identificar e evitar quaisquer perdas ou extravio de informação.

De realçar que todas as medidas constam do procedimento de suporte da gestão e entrega dos serviços de tecnologias de informação, que pode ser acedido (exclusivamente) através da TSTNet.

TST applies appropriate measures to comply with legal requirements, particularly those in the scope of security and confidentiality. TST seeks to assure the rights of the personal data owners, to guarantee their respective protection within the legal obligations that are applied to TST.

The measures will be subject to review and continuous improvement, with the IT systems being constantly monitored, aiming to prevent, identify and avoiding any loss or information leaks.

All measures are included in the procedure for management and delivery of information technology services, which can be accessed (exclusively) through TSTNet.

8. Deveres dos Visados / *Duties of Those Targeted*

Todos os visados pela Política devem reportar previamente ao Encarregado da Proteção de Dados qualquer prática de atos ou implementação de projetos e iniciativas que possam vir a ter efeitos nesta matéria em relação aos próprios, junto de terceiros ou do Concedente, por forma a que os princípios da proteção de dados possam ser aplicados desde a sua fase inicial.

Devem, ainda, reportar ao Encarregado da Proteção de Dados qualquer reclamação e/ou exercício de direitos por parte de outros Trabalhadores ou de terceiros.

Os dados pessoais a que tenham acesso deverão ser conservados como confidenciais pelas pessoas autorizadas que os tratam, não devendo ser transmitidos a terceiros sem o consentimento expresso dos seus titulares, exceto nas situações em que essa transmissão seja indispensável à prestação da atividade profissional e cumprimento de obrigações legais.

Caso tenham conhecimento da existência de qualquer incidente que possa conduzir à violação de dados pessoais ou das regras de segurança no seu tratamento deverão reportar tal situação:

- Ao Encarregado da Proteção de Dados (**gdpr@tst.com.pt**);
- À respetiva Chefia;
- Ao Helpdesk (**helpdesk@tst.com.pt**), em todos os casos que envolvam tecnologias de informação.

All those covered by this Policy must previously report to the Data Protection Officer any acts or implementation of projects and initiatives that may have effects in this matter in relation to themselves, third parties or the Grantor, so that the principles of data protection can be applied from its initial phase.

They must also report to the Data Protection Officer any complaints and/or exercise of rights by other Workers or third parties.

The personal data to which they have access must be kept confidential by the authorized persons who process them and must not be transmitted to third parties without the express consent of their owners, except in situations where such transmission is essential for fulfilment the professional activity and compliance with legal obligations.

Knowing that any incident took place that may lead to personal data breach or unfollowed security rules during the data processing, please report the incident to:

- Data Protection Officer (**gdpr@tst.com.pt**)
- Hierarchical superior
- To Helpdesk (**helpdesk@tst.com.pt**), in situations that information technologies are involved.

9. Medidas de Precaução a Adotar / *Precautions Measures to Adopt*

Todos os visados pela Política devem implementar (no mínimo) as medidas preventivas com o intuito de assegurar que, em caso de acesso a informação de carácter confidencial, são cumpridos os protocolos institucionais de forma a evitar acessos ou visualizações indevidas, quer no posto de trabalho individual, quer em reuniões, ou em outras situações:

- Não mantenha no seu local de trabalho documentação sensível que seja facilmente acedida (exemplo: deixar em cima da mesa, ou em blocos abertos). Certifique-se que a documentação está armazenada de forma segura em armários e/ou blocos de gavetas devidamente fechados e que as chaves são de acesso restrito;
- Quando está a trabalhar com documentos confidenciais nunca os deixe visíveis ou fora do seu controlo e, se os imprimir, não os deixe na impressora;
- Sempre que se ausente do computador, bloqueie a sua sessão do computador;
- Não escreva a sua password num papel, nem a partilhe. A password protege os equipamentos contra acessos indevidos;
- Em deslocações tenha especial atenção aos equipamentos móveis (Portáteis, Smartphones, tablets, pen's USB, entre outros) de modo a evitar perda ou furto;
- Os suportes físicos ou digitais que contenham dados pessoais devem ser guardados num local seguro de forma a manter em segurança a informação neles contida;
- A TST não autoriza a salvaguarda de dados pessoais em computadores e outros equipamentos de natureza pessoal (e de terceiros). Somente serão autorizados casos de exceção desde que autorizados hierarquicamente e pelo Encarregado de Proteção de Dados.
- Toda a salvaguarda de dados pessoais deve assegurar que é efetuada somente para o estrito cumprimento das suas funções profissionais (ex.: elaboração de uma chapa).
- Estes dados só devem permanecer nos equipamentos pessoais e/ou de terceiros, o tempo indispensável à realização da tarefa legítima, após o qual devem ser eliminados. Durante este tempo deve assegurar-se que o seu equipamento cumpre todas as regras básicas de segurança, tais como:
    - Encriptação dos dados através de cifra, com o auxílio de programas de uso livre como o 7-Zip e outros semelhantes;
    - A senha de acesso ao equipamento pessoal deve possuir uma dimensão mínima de 8 caracteres, deve ser memorizável, para que não tenha de ser escrita noutro local;
    - Garantir que o equipamento possui todas as atualizações de segurança mais recentes, e que não tem instalado software para além do software aprovado pela TST;
    - Seguidas regras de prudência no seguimento de hiperligações recebidas por meios não solicitados (ex.: por email). As hiperligações recebidas por email são o mecanismo mais comum para ataque a equipamentos de uso pessoal;
- Não proceder à memorização de dados acesso aos sistemas da TST, em equipamentos pessoais e/ou de terceiros (ex.: postos de internet de cafés ou hotéis, entre outros);
- A TST não autoriza o armazenamento de dados pessoais em Cloud e outros serviços públicos disponibilizados na internet, devendo ser mantidas apenas nas Cloud e serviços empresarias contratualizados pela TST, nomeadamente: Microsoft Office 365, Microsoft Teams e Microsoft Onedrive (desde que acedidos pelo acesso empresarial concedido de forma unipessoal pela TST);
- A TST não autoriza o armazenamento de dados pessoais em dispositivos portáteis de armazenamento (vulgo PEN's USB e similares), uma vez que contratualizou o uso de sistemas de armazenamento empresariais (Cloud e serviços empresariais) referidos no ponto anterior e que permitem a partilha de informação de forma protegida, dispondo ainda de uma área de rede para salvaguarda de informação de forma segura e protegida (vulgo fileshare interno).

Somente serão autorizados casos de exceção desde que autorizados hierarquicamente e pelo Encarregado de Proteção de Dados;

- A TST somente autoriza o uso da VPN empresarial para acesso aos sistemas de informação internos da TST (que não estejam disponibilizados via Internet). Quaisquer outros sistemas de acesso a computadores ou a informação armazenada internamente são de uso estritamente proibido (ex.: Anydesk, TeamViewer e similares);
- A TST exclui qualquer responsabilidade pelo uso indevido e perda de dados resultantes da utilização de equipamentos de uso pessoal e de terceiros não autorizados pela TST, e de quaisquer atividades em que se avalie que não foram aplicadas as medidas de precaução presentes na presente Política;
- A TST recomenda a configuração do segundo fator de autenticação disponibilizado através da solução Office 365 (podendo optar por um dos seguintes: endereço e-mail, número de telefone empresarial ou aplicação Microsoft Authenticator – versões android e iOS);
- A TST somente autoriza o uso da ferramenta corporativa Outlook (versões web, desktop e aplicativo para smartphone) para acesso ao e-mail corporativo, não se devendo usar outros para este efeito (ex.: gmail e semelhantes).

All those covered by this Policy must implement (at a minimum) preventive measures aiming to ensure that in the event of accessing confidential information that institutional protocols are complied with in order to avoid undie access or viewing, whether individually at the workplace, whether in meetings, or in other situations:

- Do not keep sensitive documentation in your workplace that is easily accessed (example: leaving it on the table, or in open cabinets). Make sure that the documentation is stored safely in cabinets and/or drawers that are properly closed and that the keys are restricted from general access.
- When you are working with confidential documents, never leave them visible or out of your control and, if you print them, do not leave them on the printer.
- Whenever you are away from the computer, lock your computer session.
- Do not write your password on paper or share it. The password protects equipment against unauthorized access.
- When traveling, pay special attention to mobile equipment (laptops, smartphones, tablets, USB sticks, among others) to avoid loss or theft.
- Physical or digital media containing personal data must be stored in a safe place to keep the information contained safe.
- TST does not authorize the safeguarding of personal data on computers and other equipment of personal nature (and those of third parties). Only exceptional cases will be authorized if authorized hierarchically and by the Data Protection Officer.
- Any safeguarding of personal data must ensure that it is carried out only for the strict fulfilment of their professional duties (e.g.: preparing a block or duty).
- This data must only remain on personal and/or third-party equipment for as long as is necessary to carry out the legitimate task, after which it must be deleted. During this time, you must ensure that your equipment complies with all basic safety rules, such as:
    - Encryption of data through ciphers, with the help of free-to-use programs such as 7-Zip and similar ones.
    - The password to access personal equipment must be at least 8 characters long and must be memorisable so that it does not have to be written elsewhere.
    - Ensure that the equipment has all the latest security updates, and that no software other than the software approved by TST is installed.
    - Rules of caution are followed when following links received through unsolicited means (e.g., by e-mail). Hyperlinks received by email are the most common mechanism for attacking personal equipment.
- Do not memorize applicational access to TST systems, on personal and/or third-party equipment's (e.g., internet access points in cafes or hotels, among others);
- TST does not authorize the storage of personal data in the Cloud and other public services available on the internet and must only be kept in the Cloud and business services contracted by TST, namely: Microsoft Office 365, Microsoft Teams and Microsoft Onedrive (as long as they are accessed via access business granted on a individual basis by the TST).
- TST does not authorize the storage of personal data on portable storage devices (commonly known as USB PEN's and similar devices), as it has contracted the use of corporate storage systems (Cloud and corporate services) referred to in the previous point and which allow the sharing of information in a protected manner, also having a network area to safeguard information in a safe and protected manner (known as internal fileshare). Only exceptional cases will be authorized if authorized hierarchically and by the Data Protection Officer.

- TST only authorizes the use of the corporate VPN to access TST's internal information systems (which are not available via the Internet). Any other computer access systems or information stored internally are strictly prohibited (e.g., Anydesk, TeamViewer and similar).
- TST excludes any responsibility for the misuse and loss of data resulting from the use of equipment for personal use and third parties not authorized by TST, and for any activities in which it is assessed that the precautionary measures present in this Policy were not applied.
- TST recommends configuring the second authentication factor available through the Office 365 solution (you can choose one of the following: email address, business telephone number or Microsoft Authenticator application – Android and iOS versions).
- TST only authorizes the use of the Outlook corporate tool (web, desktop and smartphone app versions) to access corporate email, and no others should be used for this purpose (e.g., Gmail and similar).

10.Atualização da Política / *Policy Update*

Quaisquer alterações à Política de Privacidade, serão disponibilizadas na página Web garantindo a divulgação das mesmas.

Any changes to the Privacy Policy will be made available on the website, ensuring their disclosure.

11.Outras Políticas e orientações / *Further Guidance*

Esta Política deve ser lida em conjunto com outras Políticas e orientações da Empresa, como a Política de Conflito de Interesses, o Código de Conduta e Ética.

This Policy should be read in conjunction with other Company Policies and guidelines, such as the Conflict-of-Interest Policy, Code of Conduct and Ethics.

12.Versões/Reviews:

Versão/*Review*	Data/*Date*	Motivo/*Reason*
1	21/11/2023	Exclusão Arriva; Revisão da Política/ *Arriva Exclusion; Policy Revision*