Política Corporativa de Proteção de Dados

Presidente Executivo

24 de novembro de 2025

CONTROLO DE VERSÕES

Versão	Data	Alterações
V1	03/03/2023	Versão inicial
V2	29/10/2024	Atualização de conteúdo
V3	24/11/2025	Revisão

CONTEÚDO

1. Objeto

A finalidade desta Política Corporativa de Proteção de Dados (doravante, a "Política") é estabelecer os princípios e diretrizes comuns e gerais de atuação que devem reger a matéria de proteção de dados pessoais para todas as empresas que compõem o Grupo Urbaser ou outras incluídas no Âmbito de aplicação, com o objetivo de promover, em qualquer caso, o cumprimento da legislação aplicável.

Em particular, a Política garante o direito à proteção dos dados de todas as pessoas físicas que se relacionam com as sociedades do Âmbito de aplicação, assegurando o respeito ao direito à honra, à privacidade e à intimidade no tratamento dos diferentes tipos de dados pessoais, provenientes de diversas fontes e com diferentes finalidades, em função da atividade empresarial desenvolvida.

2. Âmbito de aplicação

Este documento é de aplicação obrigatória à totalidade das entidades participadas (Sociedades, UTEs, Joint Ventures e outras associações equivalentes) nas quais a URBASER, S.A.U. seja o acionista maioritário ou detenha o controlo, e de cumprimento obrigatório por todo o utilizador que participe na gestão, utilização ou exploração dos dados pessoais gerados e tratados na URBASER, incluindo, mas não se limitando a, conselheiros/as, diretores/as, empregados/as, colaboradores, gestores, membros dos órgãos de governo, tudo isso sem prejuízo da legislação e dos requisitos legais específicos aplicáveis em cada país.

Nas entidades participadas em que esta Política não seja aplicável, será promovido, através dos seus representantes nos órgãos de administração, o alinhamento das suas políticas próprias com as desta Política.

IMPORTANTE: Caso exista normativa local ou setorial que contrarie o estabelecido na presente Política, cada país ou região deverá adequá-la à legislação aplicável. Tudo isso considerando que este documento contempla garantias mínimas em matéria de proteção de dados, que deverão ser respeitadas em todo momento e não poderão ser modificadas para torná-las menos eficazes.

3. Conteúdo

- **Princípios e considerações gerais relativas ao tratamento de dados pessoais.**

A legislação aplicável em matéria de proteção de dados será rigorosamente cumprida, em função do tratamento de dados pessoais que for realizado e do que for determinado de acordo com as normas ou procedimentos adotados no seio do Grupo.

Além disso, será promovida a observância dos princípios e considerações estabelecidos na presente Política: (i) na conceção e implementação de procedimentos que envolvam o tratamento de dados pessoais; (ii) nos produtos e serviços oferecidos; (iii) na contratação de serviços que impliquem o tratamento de dados pessoais e; (iv) na implementação de quaisquer sistemas e plataformas que permitam o acesso por parte dos profissionais do Grupo ou de terceiros a dados pessoais e à recolha ou tratamento desses dados.

De acordo com o acima exposto, qualquer tratamento de dados pessoais realizado no Grupo deverá observar os seguintes princípios e considerações gerais:

a) Princípios de legitimidade, licitude e lealdade no tratamento de dados pessoais

O tratamento de dados pessoais será legítimo, lícito e leal. Neste sentido, só poderá ser realizado um tratamento de dados pessoais quando existir uma base legal que o habilite, como o consentimento do interessado, o contrato de trabalho, o cumprimento de obrigações legais, o interesse público ou os interesses legítimos perseguidos pelo Responsável pelo tratamento, respeitando sempre os direitos e liberdades dos interessados.

Esta habilitação legal deve ser documentada, garantindo a sua disponibilidade para revisão e auditoria.

Além disso, os dados pessoais devem ser tratados de forma justa e leal, o que implica que a entidade não os pode utilizar de

forma enganosa ou fraudulenta.

Não serão recolhidos nem tratados dados pessoais relativos à origem étnica ou racial, à ideologia política, às crenças, às convicções religiosas ou filosóficas, à vida ou orientação sexual, à filiação sindical, à saúde, nem dados genéticos ou biométricos destinados a identificar de forma unívoca uma pessoa, a menos que exista uma autorização legal de acordo com a regulamentação de proteção de dados e/ou regulamentação local aplicável, caso em que deverá ser comprovado que o tratamento é necessário, legítimo e proporcional, não existindo métodos alternativos com os quais se possa satisfazer a mesma finalidade.

b) Princípio da minimização

Apenas serão objeto de tratamento os dados pessoais que sejam estritamente necessários para a finalidade para a qual são recolhidos, ou seja, serão adequados, pertinentes e limitados ao necessário em relação aos fins para os quais são tratados.

c) Princípio da exatidão

Os dados pessoais devem ser exatos e atualizados, sendo tomadas medidas razoáveis para que o interessado possa solicitar a sua retificação ou supressão, quando for o caso.

d) Princípio da limitação da finalidade e do prazo de conservação

Os dados pessoais serão recolhidos para fins específicos, explícitos e legítimos e não serão posteriormente tratados de forma incompatível.

O tratamento posterior dos dados pessoais para fins de arquivo de interesse público, fins de investigação científica e histórica ou fins estatísticos não será considerado incompatível com os fins iniciais, desde que os restantes princípios sejam tidos em conta.

Além disso, os dados pessoais não serão conservados para além do prazo necessário para atingir a finalidade para a qual foram recolhidos, salvo nos casos previstos na lei.

e) Princípios de integridade e confidencialidade

No tratamento dos dados pessoais deve ser garantida, através de medidas técnicas e organizacionais, uma segurança adequada que os proteja do tratamento não autorizado ou ilícito e que evite a sua perda, destruição e/ou danos acidentais.

Os dados pessoais recolhidos e tratados pelas entidades do Grupo devem ser conservados com a máxima confidencialidade e sigilo, não podendo ser utilizados para outros fins que não aqueles que justificaram e permitiram a sua recolha, sem que possam ser comunicados ou cedidos a terceiros fora dos casos permitidos pela legislação aplicável.

f) Princípio da responsabilidade proativa (prestação de contas)

As entidades do Grupo serão responsáveis pelo cumprimento dos princípios estipulados nesta Política e exigidos pela legislação aplicável, devendo ser capazes de o demonstrar.

Para tal, serão previamente avaliados os riscos que novos tratamentos, produtos, serviços ou sistemas de informação podem acarretar para a proteção de dados pessoais e serão adotadas as medidas necessárias para os eliminar ou mitigar. Nos casos em que a lei o exigir, deverá ser realizada uma avaliação do risco dos tratamentos que envolvam um risco elevado para os direitos e liberdades dos interessados, a fim de determinar as medidas a aplicar para garantir que os dados pessoais sejam tratados de acordo com as exigências legais.

Além disso, deverá ser mantido um registo ou inventário de atividades que descreva os tratamentos de dados pessoais realizados no âmbito das suas atividades.

Nos casos previstos na lei, serão designados delegados de proteção de dados ("DPD"), com o objetivo de garantir o cumprimento da regulamentação de proteção de dados nas entidades do Grupo. Na ausência de DPD, poderão ser designados Coordenadores de Proteção de Dados.

g) Princípios de transparência e informação

O tratamento de dados pessoais será transparente em relação à pessoa em causa, fornecendo-lhe informações sobre o tratamento dos seus dados de forma compreensível e acessível.

A fim de garantir um tratamento leal e transparente, a entidade do Grupo responsável pelo tratamento deverá informar as pessoas afetadas ou interessadas cujos dados se pretende recolher, nomeadamente:

- a identidade e os dados de contacto do responsável pelo tratamento;

- a finalidade do tratamento dos dados;
- os terceiros ou categorias de terceiros a quem os dados são transferidos, se for o caso;
- a base jurídica do tratamento;
- os direitos de proteção de dados que podem ser exercidos pelos interessados.
- a intenção de realizar transferências internacionais, se for o caso;
- o prazo de conservação dos dados;
- os dados de contacto do Delegado de Proteção de Dados, se for o caso..

h) Aquisição ou obtenção de dados pessoais

É proibida a aquisição ou obtenção de dados pessoais de fontes ilegítimas, de fontes que não garantam suficientemente a sua proveniência legítima ou de fontes cujos dados tenham sido recolhidos ou cedidos em violação da lei.

i) Contratação de responsáveis pelo tratamento

Antes de contratar qualquer prestador de serviços que tenha acesso a dados pessoais sob a responsabilidade das entidades do Grupo, bem como durante a vigência da relação contratual, devem ser tomadas as medidas necessárias para garantir um nível de segurança adequado.

Da mesma forma, uma vez verificado um nível adequado de segurança do prestador de serviços que terá acesso aos sistemas de informação de qualquer uma das empresas que compõem o Grupo, serão assinados os contratos correspondentes de tratamento de dados pessoais, nos casos em que for aplicável..

j) Transferências internacionais de dados

Quando um tratamento implicar uma transferência internacional de dados pessoais para um país terceiro ou organização internacional que não ofereça o mesmo nível de garantias, deverão ser adotadas as medidas necessárias com o objetivo de reforçar a segurança dos dados pessoais, de modo que só poderá ser realizada mediante o estabelecimento de garantias adequadas.

Da mesma forma, as entidades do Grupo localizadas fora do Espaço Económico Europeu devem cumprir os requisitos estabelecidos para as transferências internacionais de dados pessoais que sejam, se for o caso, aplicáveis na sua jurisdição.

k) Direitos das pessoas interessadas

As entidades do Grupo deverão permitir que as pessoas interessadas possam exercer os direitos de acesso, retificação, supressão, limitação do tratamento, portabilidade e oposição aplicáveis em cada jurisdição, estabelecendo, para esse efeito, os procedimentos internos necessários.

l) Brechas de segurança

No caso de ocorrer um incidente que provoque a destruição, perda ou alteração acidental ou ilícita de dados pessoais, ou a comunicação ou acesso não autorizado a esses dados, deverá ser seguida a Política Corporativa de Segurança da Informação do Grupo, bem como os procedimentos internos que a desenvolvem. Esses incidentes deverão ser documentados e serão tomadas medidas para resolver e mitigar os possíveis efeitos negativos para os interessados.

m) Registo de Atividades de Tratamento

Deve ser mantido um registo ou inventário onde sejam descritas todas as atividades desenvolvidas na organização que envolvam o tratamento de dados pessoais.

Desta forma, todas as empresas do Grupo deverão manter um inventário que inclua, no mínimo, o conjunto de atividades de tratamento, finalidades e sua correspondente descrição, tipologia de dados tratados e outra série de questões relacionadas com o tratamento de dados pessoais realizado pelo responsável.

4. Implementação

Com o objetivo de garantir o cumprimento da presente Política, cada empresa do Grupo dedicará os recursos adequados para

a sua implementação, manutenção e revisão, e desenvolverá os procedimentos internos de caráter local necessários para concretizar o seu conteúdo, adaptando-o às novidades normativas que possam surgir, sempre em conformidade com a política e os procedimentos corporativos.

5. Formação

Serão promovidas as medidas de formação e sensibilização necessárias para o conhecimento e a cultura em matéria de proteção de dados, que deverão ser ministradas periodicamente, com o objetivo de aumentar os conhecimentos dos funcionários, em particular daqueles que têm acesso aos sistemas de informação.

6. Controlo e supervisão

O Delegado de Proteção de Dados supervisionará o cumprimento do disposto nesta Política, em conjunto com os diferentes Coordenadores de Proteção de Dados designados a nível nacional e internacional, que serão responsáveis por estabelecer e implementar procedimentos internos de caráter local, adaptando o seu conteúdo em função da legislação aplicável nas suas respetivas jurisdições.

7. Dúvidas, comunicações ou reclamações

As consultas no âmbito desta Política devem ser dirigidas ao Departamento Corporativo de Cibersegurança e Proteção de Dados da URBASER para o endereço habilitado: pdp@urbaser.com.

Qualquer incidente relacionado com o incumprimento do estabelecido nesta Política e procedimentos relacionados, ou a sua conformidade com o estabelecido no Código de Conduta do Grupo, deve ser dirigido ao órgão de conformidade regulamentar correspondente através do Canal Ético constante da página web do Grupo (www.urbaser.com).

8. Incumprimentos

A presente Política é considerada uma norma de cumprimento obrigatório, pelo que a sua violação constituirá uma infração da mesma e a Empresa adotará as medidas disciplinares, contratuais ou legais que forem pertinentes, sem prejuízo de outras responsabilidades em que o infrator possa ter incorrido. Da mesma forma, a URBASER reserva-se o direito de adotar as medidas que considerar oportunas contra os parceiros comerciais que a infringirem. Qualquer exceção ou isenção, seja por motivos organizacionais, legais, contratuais, tecnológicos ou de outra natureza, a esta Política ou a qualquer norma, procedimento ou instrução técnica da qual ela dependa, será gerida de acordo com os documentos internos definidos para tal.

9. Revisão e atualização

O Departamento Corporativo de Cibersegurança e Proteção de Dados reverá periodicamente o conteúdo desta Política Corporativa, garantindo que ela reflita as recomendações e melhores práticas em vigor, e proporá ao Comitê de Segurança da Informação as modificações e atualizações que contribuam para o seu desenvolvimento, aprovação e melhoria contínua.

www.urbaser.com