

dot2web

Alojamento de sites
e registo de domínios.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

Índice

1. Introdução.....	2
2. Dados pessoais.....	2
3. Registo de domínios – política de WHOIS	4
4. Medidas de segurança.....	5
5. Fugas de informação e falhas de segurança – Data Breaches.....	6
6. Divulgação responsável de vulnerabilidade	7
7. Questões ou dúvidas.....	7
8. Alterações e atualizações	7
9. Entidade responsável pelo tratamento de dados pessoais	7

1. Introdução

Com a entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD), a gestão e proteção de dados pessoais passará a ser uma prioridade para todas as empresas que atuem na União Europeia.

A Olivertek Lda, adiante designada Dot2web, A Dot2web é um provedor de alojamento web e disponibiliza ao cliente serviços informáticos ligados à Internet, onde se incluem o alojamento de sites em ambiente partilhado, servidores dedicados, servidores privados, housing, registo de domínios, certificados digitais de segurança e segurança de sites e desenvolvimento de software.

Neste documento encontrará as principais medidas e procedimentos associados à implementação do regulamento por parte da Dot2web, no que se refere à proteção de dados pessoais dos seus clientes.

Em relação ao RGPD, a Dot2web assume os seguintes papéis e responsabilidades no que se refere à proteção de dados pessoais:

- **Controlador (Data controller)** enquanto responsável pelo controlo de todos os dados que recolhe dos seus clientes, para prestação dos serviços contratados e respetivo suporte;
- **Processador (Data processor)** enquanto provedor de alojamento web, prestador de serviço online, registo de domínios ou venda de certificados SSL.

Para além das informações constantes neste documento, deverá também ter em consideração os seguintes documentos:

- Termos e condições específicas para o registo de domínios (TCERD) - Regras para registo de domínios;
- Condições específicas para a prestação de serviços de servidores (CESS) - Restrições e regras relativas ao alojamento de dedicado em servidores Virtuais e servidores Dedicados;
- Condições particulares (CP) – Detalhe das características dos serviços contratados e disponíveis em <https://www.dot2web.pt> e <https://my.dot2web.pt> ;
- Política de privacidade (PP) – Detalhe sobre recolha e registo de dados;

2. Dados pessoais

2.1. Recolha, consentimento e finalidade de tratamento

Todos os dados armazenados nos nossos servidores foram recebidos com base na contratação do serviço pelo cliente e manter-se-ão pelo período da duração do contrato. Sempre que se aplique ao serviço contratado, manter-se-á, durante o tempo definido no contrato os backups dos conteúdos anteriormente alojados.

A Dot2web garante que o consentimento da recolha de dados, no ato do preenchimento da ficha de cliente ou de formulários de contacto, é obtido de forma ativa e consciente solicitando os dados necessários para efeitos legais e correta prestação do serviço para os quais são recolhidos.

Fora o consentimento e para a execução de um acordo, contrato, proposta ou documento digital é necessário e indispensável o tratamento dos dados recolhidos.

Todos os dados recolhidos e tratados pela Dot2web encontram o seu fundamento e necessidade intrínseca para a prestação do(s) serviço(s) subscrito(s).

A Dot2web apenas trata os dados recolhido mediante consentimento do cliente, sendo os restantes fornecidos de forma voluntária excluídos e ignorados.

2.2. Direito de acesso

Poderá aceder, corrigir e alterar os dados de que é titular através da sua área de cliente reservada, disponível <https://my.dot2web.pt>.

Exclui-se o acesso de dados ou alteração dos mesmos quando:

- Acesso e/ou alteração de dados solicitada por outras vias que não a área de cliente;
- Quando não exista acesso ao email autorizado

Caso o cliente não tenha acesso ao email autorizado, deverá solicitar alteração de email autorizado através de preenchimento de formulário com dados de identificação, os quais serão verificados pela Dot2web para efeitos de confirmação legal. Apenas após aceitação do pedido de alteração pela Dot2web, procederemos à alteração dos dados. Este formulário encontra-se disponível em <https://dot2web.pt/legal>. A Dot2web manterá o formulário de pedido de alteração de contacto, armazenado e com acesso restrito para efeitos de evidência.

2.3. Direito à portabilidade

O titular dos dados poderá solicitar à Dot2web uma cópia dos seus dados em formato de uso comum. Este pedido deverá ser solicitado por email autorizado para rpgd@dot2web.pt.

A Dot2web, desconhece os conteúdos alojados nos seus servidores e limita-se a permitir o acesso aos seus clientes para que possam migrar os conteúdos alojados nos seus servidores para qualquer outro provedor de serviços ou dispositivo de armazenamento.

2.4. Direito ao esquecimento

O titular dos dados pessoais terá o direito de ver os seus dados eliminados e interrompido o seu tratamento quando:

- O propósito para o qual os dados foram recolhidos deixe de existir, e os dados em si deixem de ser necessários para nenhum fim que lhe seja conhecido ou transmitido;
- Quando não existe consentimento do titular independentemente do fim;
- Quando não exista sustentação legal para tal;
- Em qualquer caso em que os dados sejam tratados em violação do RGPD.

A Dot2web poderá negar-se à eliminação ou alteração dos dados, quando estes correspondam a obrigações contratuais e em defesa dos seus interesses legítimos, bem como o cumprimento da lei, nomeadamente a lei fiscal. Nestes casos, restringirá o acesso e tratamento desses mesmos dados como forma de preservá-los como evidência, mantendo-os armazenados, não tratados, e apenas com acesso restrito e justificado.

Além dos titulares dos dados que exerçam o seu direito ao esquecimento, também todos aqueles que apresentam mais de 1 ano de inatividade passarão automaticamente a ser armazenados em conformidade.

Em relação aos dados alojados nos nossos servidores e de acordo com o serviço contratado, a limitação ao esquecimento está intrinsecamente ligada ao tempo obrigatório de retenção de backups.

A Dot2web, não poderá ainda apagar qualquer dado quando não haja ordem expressa do controlador ou da autoridade judiciária com poderes para o ato.

2.5. Pseudonimização e anonimização

A Dot2web utiliza pseudonimização e anonimização não sendo autorizado ao normal operador o acesso a dados pessoais, exceto e-mail autorizado para identificação do cliente.

2.6. Criação de perfil

Não efectuamos tratamento automatizado, incluindo a definição de perfis que produzam decisões com efeitos jurídicos.

2.7. Privacy by design, privacy by default e Data Minimization

É obrigação no âmbito do RGPD garantir a privacidade e proteção dos dados pessoais desde a conceção (de produto ou serviço) e durante todo o tempo em que se processe ou controle dados pessoais, levando à minimização da exposição de risco.

A Dot2web cumpre com os requisitos inerentes ao que se entende por privacy by design e by default, usando os meios de segurança adaptados, com certificados de segurança e pseudonimização desde a subscrição de serviço, encriptação de dados, firewall, antivírus & Antimalware, acessos autenticados por VPN controlados e restritos assim como uma ferramenta de Data Control.

2.8. Segurança de Dados de Pagamento

Alguns dos modos de pagamento disponibilizados pela Dot2web são processados por terceiros.

Quando o cliente seleciona pagamento por Paypal, a Dot2web passa a solicitação para o website da Paypal onde a transação ocorre. Portanto, os dados de pagamento não são armazenados nos nossos sistemas.

A Paypal efetua transações financeiras online em milhares de empresas em todo o mundo e está em conformidade com os padrões PCI-DSS para armazenamento e tratamento de informações de pagamento.

3. Registo de domínios – política de WHOIS

A propriedade de um domínio é identificada publicamente pelo WHOIS, com dados pessoais como nome, morada, contacto telefónico e email.

Para todos os domínios registados em nome individual ativaremos por defeito o WHOIS privado. Os seus dados pessoais apenas serão disponibilizados no WHOIS caso seja do seu interesse e mediante consentimento expresso através de um documento disponível para download na nossa área de cliente. A solicitação de WHOIS público deverá ser efetuada através do contacto rgpd@dot2web.pt.

Relembramos que mesmo com WHOIS privado a titularidade do domínio estará salvaguardada, no entanto, os seus dados pessoais não são disponibilizados publicamente nos motores de pesquisa de WHOIS, ou serão substituídos por dados fictícios.

Os dados pessoais recolhidos para efeitos de registo de domínios são cedidos à entidade registrar competente. Em todos os casos, serão solicitadas informações relacionadas com o cumprimento com o RGPD, para que possamos garantir que os dados dos nossos clientes estão devidamente protegidos.

Adicionalmente, consulte ainda Termos e condições específicas para o registo de domínios (TCERD) - Regras para registo de domínios, disponível em <https://dot2web.pt/legal>.

4. Medidas de segurança

4.1. Rede empresarial interna

Todos os nossos serviços são geridos através da nossa rede empresarial interna que dispõe de medidas de segurança apropriadas para garantir a proteção de dados dos nossos clientes, assim como a segurança de gestão da nossa infraestrutura:

- Software antivírus em todos os equipamentos internos, que disponibiliza proteção contra malware;
- Rede wi-fi empresarial protegida por password não cedida a visitantes;
- Backups diários de bases de dados de clientes;
- Encriptação de equipamentos internos;
- SIEMFeeder em todos equipamentos (Security information and event management)

4.2. Websites

As comunicações efetuadas através dos websites geridos pela Dot2web são efetuadas por TLS/SSL (HTTPS), garantindo a encriptação da comunicação entre o seu browser e os nossos servidores.

4.3. Infraestrutura e rede de servidores

4.3.1. Segurança Física

O nosso Datacenter localiza-se num dos maiores e mais conceituados provedores de Datacenter em Portugal. Todos os recursos do provedor são aproveitados para proteger a nossa infraestrutura contra ameaças ou impactos físicos. O datacenter possui controlo de acessos e vigilância local e remota 24x7 para proteger contra entrada não autorizada. Os controlos de segurança fornecidos pelas nossas instalações de datacenter incluem, mas não estão limitados:

- Serviço de segurança física 24x7;
- Sistema de controlo de acessos a pessoas autorizadas;
- Controlo de acessos por cartão e autenticação biométrica;
- Sistema de vídeo vigilância;
- Estrutura antissísmica;
- Infraestrutura automática de deteção e combate a incêndios;
- Sistema AVAC (controlo de temperatura e humidade);
- Portas blindadas e anti-fogo;
- Energia elétrica protegida por UPS e geradores;

O Datacenter é ainda certificado pela ISO9001 e ISO27001.

4.3.2. Segurança de Infraestrutura

O acesso à gestão de infraestrutura é efetuado por sistemas de autenticação multi-factor (2FA).

O acesso aos nossos equipamentos é baseado em políticas de grupo sendo que é atribuído apenas o acesso estritamente necessário para a intervenção do equipamento.

Consideramos qualquer sistema que armazene os dados dos nossos clientes como sistemas altamente sensíveis sendo o acesso a estes sistemas limitado e monitorizado.

Os discos rígidos e infraestrutura são apagados com segurança antes de serem desativados ou reutilizados para garantir a completa segurança dos seus dados.

4.3.3. Registo de Logs

Os nossos sistemas de segurança e monitorização efetuam o registo de logs para permitir a monitorização de desempenho e segurança. O registo inclui ações do sistema, bem como os logins e comandos emitidos pelos nossos administradores de sistemas.

4.3.4. Monitorização de Segurança

Toda a infraestrutura é controlada 24x7x365 por uma equipa técnica certificada e altamente especializada. A nossa infraestrutura encontra-se integrada num sistema de monitorização e alarmística permanente que controla todo o equipamento físico, sistemas, plataformas e serviços.

A nossa equipa técnica recorre a processos de monitorização e análise para identificar atividades potencialmente maliciosas na nossa infraestrutura. Os comportamentos do utilizador e dos sistemas são monitorizados no sentido de identificar atividades suspeitas, e as investigações são realizadas seguindo os procedimentos de resposta a incidentes.

Não obstante as medidas de segurança implementadas, não nos responsabilizamos pela perda de dados de acesso a serviços de alojamento ou e-mails, que possam ter como consequência o acesso a dados e ou informação por pessoas não autorizadas. A garantia de proteção dos dados de acesso aos serviços são da responsabilidade do cliente de acordo com termos e condições contratuais. É, no entanto, prática da Dot2web, monitorizar e comunicar ao cliente quando possíveis contas de email ou websites possam ter sido comprometidos ou apresentem atividade suspeita.

4.3.5. Backups e Snapshots.

A Dot2web faz backups diários em servidores remotos de forma a evitar catástrofes. Estes backups, assim como toda a rede de gestão de infraestrutura são geridos por redes internas e isoladas, não passando este tráfego pela internet. Estes backups são alojados em servidores isolados e totalmente encriptados.

5. Fugas de informação e falhas de segurança – Data Breaches

A violação de dados pessoais é definida no RGPD como “uma violação de segurança que leva à destruição accidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados, ou processados de outra forma”.

Violações de dados pessoais podem ser divididos em três tipos, sendo que uma só violação de dados pode envolver, uma, duas ou até as três categorias, a saber:

- Violação de confidencialidade, quando haja divulgação ou acesso não autorizado ou accidental a dados pessoais;
- Violação de disponibilidade, quando houve uma perda de acesso ou destruição de dados pessoais;
- Violação de integridade, quando haja alteração não autorizada ou accidental de dados pessoais.

Com o RGPD mais que responsabilidade por evitar que as violações de segurança aconteçam, passa ainda a existir a obrigação legal de verificar a gravidade da violação e notificar a autoridade supervisora. A comunicação à entidade supervisora e envio de relatório deverá ser efetuada no máximo de 72 horas após tomada de conhecimento da violação de dados.

São excluídos da necessidade de comunicação as violações dos dados pessoais que não sejam suscetíveis de resultar num risco para os direitos e liberdades dos indivíduos tendo um efeito prejudicial significativo sobre os indivíduos afetados.

Também o titular deve ser notificado em linguagem clara e simples com explicação concreta da ocorrência. Exclui-se da obrigação de notificação do titular quando as medidas de proteção técnicas e organizacionais aplicadas tornem os dados pessoais inteligíveis a qualquer pessoa não autorizada a aceder-lhes, como a pseudonimização ou anonimização, ou caso tome medidas subsequentes que afastem o risco de afetação os direitos e liberdades dos titulares dos dados.

A Dot2web preocupa-se com os dados pessoais dos seus clientes e tenta ao máximo implementar medidas técnicas e organizacionais que evitem a fuga de informação e violação de dados pessoais.

Em todo o caso, estão a ser adotados procedimentos de comunicação para garantir uma eficaz comunicação à entidade supervisora e notificação ao titular dos dados, assim como a implementação de medidas preventivas para evitar esta necessidade.

Antes de qualquer tipo de comunicação e notificação, efetuaremos uma análise de risco do incidente, agindo em conformidade.

6. Divulgação responsável de vulnerabilidade

Trabalhamos diariamente na identificação de novas soluções e implementação de melhorias na nossa infraestrutura.

Se detetou alguma vulnerabilidade contacte a nossa equipa técnica e envie os detalhes da mesma para suporte@dot2web.pt.

As vulnerabilidades submetidas serão analisadas, triadas e em seguida avaliadas em detalhe para determinar o nível de risco. As vulnerabilidades de segurança são tratadas com a máxima importância para garantir a segurança dos seus dados pessoais e a segurança dos nossos serviços.

Divulgar publicamente uma vulnerabilidade pode colocar em risco toda a nossa infraestrutura.

7. Questões ou dúvidas

Para qualquer dúvida, esclarecimento sobre a segurança dos seus dados pessoais ou alojados nos nossos servidores envie-nos um email para rgpd@dot2web.pt.

8. Alterações e atualizações

Numa perspetiva de melhoria contínua, reservamo-nos o direito de, a qualquer altura, proceder a reajustamentos ou alterações às medidas e procedimentos de segurança e proteção de dados pessoais identificadas neste documento.

9. Entidade responsável pelo tratamento de dados pessoais

A Olivertek Lda, designada por Dot2web, com centro de operações em Portugal, na Rua S. Lourenço, nº 12, 1º andar sala AO, 4445-596 Ermesinde.

Para efeitos de esclarecimento, dúvidas ou questão por favor utilizar o seguinte contacto rgpd@dot2web.pt.