GOVERNO DO DISTRITO FEDERAL

1. Conceito de Privacy by Design

O **Privacy by Design (PbD)** promove a integração de privacidade em todas as fases do desenvolvimento de sistemas e serviços, visando proteger os dados pessoais desde a concepção. Esse conceito, proposto por Ann Cavoukian, foi amplamente adotado para fortalecer a proteção dos direitos e liberdades dos indivíduos.

2. Princípios Fundamentais do Privacy by Design

Sete princípios orientam a implementação do Privacy by Design:

1. **Proativo, não reativo**: antecipa riscos de privacidade para evitá-los antes de ocorrerem.
2. **Privacidade como padrão**: os sistemas devem proteger automaticamente a privacidade, sem a necessidade de configuração pelo usuário.
3. **Privacidade integrada ao design**: a proteção de dados é incorporada ao design e ao funcionamento dos sistemas, não como um acessório.
4. **Funcionalidade total**: soluções que protejam a privacidade sem comprometer a funcionalidade.
5. **Segurança de ponta a ponta**: garante proteção durante todo o ciclo de vida dos dados.
6. **Visibilidade e transparência**: processos claros e auditáveis para demonstrar conformidade.
7. **Respeito pela privacidade do usuário**: sistemas centrados no usuário, permitindo que eles tenham controle sobre seus dados.

3. Requisitos de Privacidade para Sistemas

Para assegurar a proteção de dados, os sistemas devem atender a três metas de segurança:

- **Confidencialidade**: previne o acesso não autorizado.
- **Integridade**: protege contra alterações não autorizadas.
- **Disponibilidade**: garante que os dados estejam acessíveis conforme necessário.

Adicionalmente, são considerados três objetivos de privacidade:

- **Desvinculação**: impede a conexão de dados entre diferentes contextos.
- **Transparência**: promove clareza nos processos e acesso à informação sobre o uso de dados.
- **Intervenção**: assegura que o usuário possa intervir no tratamento dos dados e exercer seus direitos.

4. Estratégias de Design para Privacidade

São identificadas oito estratégias, divididas entre orientadas a dados e a processos:

- **Estratégias orientadas a dados**:
  - **Minimizar**: coleta e processamento do mínimo de dados.
  - **Ocultar**: limita a observabilidade dos dados, incluindo técnicas de criptografia.
  - **Separar**: evita a vinculação de dados de diferentes fontes.

- **Abstrair**: reduz o nível de detalhamento dos dados.

- **Estratégias orientadas a processos**:
  - **Informar**: assegura que os titulares estejam cientes do tratamento dos seus dados.
  - **Controlar**: permite que os titulares exerçam controle sobre seus dados.
  - **Impor**: cumpre os requisitos legais e políticas de proteção.
  - **Demonstrar**: possibilita a demonstração de conformidade com requisitos de privacidade.

5. Padrões de Design e Tecnologias para Aperfeiçoamento da Privacidade (PETs)

Padrões de design e tecnologias de aprimoramento de privacidade (Privacy Enhancing Technologies, PETs) são aplicados para solucionar problemas comuns de privacidade. Esses padrões incluem práticas como anonimização, pseudonimização e criptografia. Já as PETs consistem em ferramentas e soluções tecnológicas para implementar as estratégias de privacidade e proteger dados em sistemas complexos.

6. Conclusão

A implementação do Privacy by Design é essencial para a criação de sistemas que respeitem a privacidade e garantam a conformidade com regulamentações de proteção de dados. Esses princípios e estratégias ajudam a construir uma cultura de privacidade, colocando o indivíduo no centro do processamento de dados.