DECISÃO

Data: 16 Janeiro 2017
Referência: 2017-001
Emitido por: Secretaria Geral
Contato: Jacques Perret E-Mail: jacques.perret@engie.com Tel.:+33 (0)1 44 22 50 17

Política de Privacidade de Dados do Grupo

Esta decisão descreve a Política de Privacidade de Dados do Grupo ENGIE aplicável a todas as entidades do Grupo. Quando necessário, devido à legislação local, esta política poderá ser adaptada.

Esta política está baseada na versão adotada em janeiro de 2014 e foi atualizada principalmente em decorrência dos seguintes eventos:

- A reorganização do Grupo em janeiro de 2016;
- As conclusões de auditoria que recomendou o fortalecimento da governança neste âmbito;
- A adoção da Regulamentação de Proteção Geral de Dados da União Europeia - UE.

Esta política define os princípios e objetivos, a organização e o sistema de monitoramento que foram implementados com relação à proteção de dados pessoais.

Esta decisão, aprovada no Comitê Executivo de 9 de janeiro de 2017, entra em vigor imediatamente.

Jacques Perret Group Data Privacy Officer

Pierre Mongin
Group General Secretary

Isabelle Kocher
Chief Executive Officer

Esta decisão entra em vigor a partir de 16 Janeiro de 2017.

Documento (s) cancelados ou alterados: Política de privacidade de dados do Grupo (Janeiro 2014)
Anexo (s): Texto
Distribuição: Texto

ERRATA:

De acordo com as orientações[1] da WP29, o termo “Diretor de Proteção de Dados” ou “Data Privacy Officer”, usado nessa Política para todas as BUs e Entidades é substituído por “Gestor de Privacidade de Dados” ou “Data Privacy Manager”.

“Diretor de Proteção de Dados - DPD” é usado apenas em referência àqueles designados para a Autoridade de Proteção de Dados.

Como consequência, por favor veja em anexo o adendo e a atualização da Política de Privacidade de Dados do Grupo.

Abril de 2017.

[1] Diretrizes sobre "Diretores de Proteção de Dados" publicadas pelo Grupo de Trabalho do Artigo 29 (WP29). O WP29 é composto por um representante da Autoridade de proteção de dados de cada Estado-Membro da UE, a Autoridade Europeia de Proteção de Dados e a Comissão Europeia.

1. Contexto, temas e desafios

O Grupo está profundamente comprometido com a proteção de Dados Pessoais e da privacidade pessoal, que são valores estabelecidos em nosso Código de Ética.

O Grupo Engie processa Dados Pessoais relacionados a seus empregados, clientes, parceiros, prestadores de serviço e fornecedores, no curso de suas atividades diárias (administração de pessoal, prospecção e gestão de soluções para clientes, etc.)

As pessoas estão cada vez mais conscientes dos dados que partilham, e desta forma, esperam uma proteção e tratamento apropriados aos seus Dados Pessoais.

As autoridades públicas estão cada vez mais conscientes destes assuntos. Elas estão impondo obrigações mais rigorosas sobre as empresas que processam Dados Pessoais e podem impor sanções civis, criminais e financeiras. Assim, o Grupo e suas Entidades devem se adaptar a essas regras[2].

Consequentemente, o Grupo se encontra cada vez mais exposto aos riscos relacionados com a coleta, uso, modificação inapropriados, internos ou externos, com a exposição e mesmo a falsificação de Dados Pessoais.

Baseado em seus valores éticos relacionados a dados pessoais e privacidade, e plenamente consciente da importância das regras sobre a proteção de dados, privacidade e os riscos envolvidos em eventual violação de dados, o Grupo assume o dever de proteger tais dados e a privacidade, motivo pelo qual implanta a presente política (a “Política”).

2. Escopo e objetivos

A Política está alinhada com o Código de Ética do Grupo, e sua abordagem de gerenciamento de risco e proteção de Patrimônio[3].

Os princípios desta Política estão baseados nas convenções internacionais listadas no anexo 3. No caso de qualquer conflito entre a Política e as convenções internacionais aplicáveis ou as regras nacionais aplicáveis a uma Entidade, esta última terá preferência sobre estes princípios.

A Política de Privacidade de Dados do Grupo aplica-se a todo o seu pessoal e Entidades.

Esta Política será reforçada e tornada mais detalhada com a inclusão progressiva de outros documentos (metodologias, procedimentos, boas práticas, conscientização, etc.) que possibilitarão os objetivos estabelecidos.

As exigências a seguir deverão ser atendidas anteriormente à real implementação de qualquer Processamento de Dados e será levada em consideração no planejamento de qualquer projeto envolvendo processamento de Dados Pessoais. Uma vez implementado, o Processamento de Dados deverá, a todo o tempo, respeitar os princípios estabelecidos nesta Política. Exigências semelhantes também podem se aplicar no caso de uma mudança nas condições sob as quais é realizado o Processamento de Dados.

[2] Regulamento da UE de 2016/679 de 27/04/2016 sobre a proteção das pessoas naturais com relação ao processamento de Dados Pessoais e ao livre movimento destes dados (vigente a partir de 25 Maio de 2018 e incorrendo em penalidade entre 2 e 4% do volume total global de faturamento do ano financeiro anterior, a ser imposto às Entidades responsáveis por infringir as disposições do Regulamento).
[3] Cf. Política de Proteção de Patrimônio do Grupo (Janeiro 2016).

3. Governança

Os objetivos e meios de proteção de Dados Pessoais descritos abaixo devem ser implementados a nível de Grupo, em cada BU, suas Entidades, e centros de serviço compartilhados.

3.1. A Nível do Grupo

O gerenciamento estratégico da Política de Privacidade de Dados do Grupo é responsabilidade do Comitê Executivo da ENGIE, o qual delega a coordenação e o gerenciamento operacional da Política ao Secretário Geral do Grupo, o qual por sua vez delega esta tarefa ao Gestor de Proteção de Dados do Grupo.

O Gestor de Proteção de Dados do Grupo deve ser notificado sobre qualquer dificuldade na implementação desta Política.

3.1.1 Gestor de Proteção de Dados do Grupo

As principais tarefas do Gestor de Proteção de Dados do Grupo são garantir uma implementação efetiva desta Política e coordenar as atividades relacionadas com os GPDs das BUs (ver Apêndice 2).

3.1.2. O Comitê de Privacidade

Esta Política estabelece um Comitê de Privacidade para gerenciar atividades transversais relacionadas à Proteção de Dados.

O Comitê de Privacidade, dirigido pelo Gestor de Proteção de dados do Grupo, reunirá todos Gestores de Proteção de Dados das BUs, trimestralmente. O Comitê também incluirá um representante de cada um dos seguintes Departamentos: Departamento de Ética & Conformidade, Departamento de Auditoria e Riscos, Departamento de Controle Interno e Departamento de Recursos Humanos, assim como incluirá, caso necessário, o Diretor de Segurança Cibernética e Informação do Grupo e o Diretor de Segurança do Grupo, atuando como representante do Comitê de Segurança da Informação.

O Comitê de Privacidade decide as ações transversais no seu nível e as submete aos órgãos ou instâncias a nível de Grupo, e caso necessário, ao Comitê Executivo da ENGIE para aprovação.

O Comitê de Privacidade é responsável pelo Sistema de Gerenciamento de Privacidade de Dados, cuja finalidade principal é verificar a conformidade com a Política de Privacidade de Dados do Grupo.

Uma vez ao ano, o Comitê de Privacidade irá elaborar um relatório de suas atividades (incluindo uma revisão da implementação desta Política) e irá apresentar tal relatório aos órgãos relevantes do Grupo.

3.2. A nível da BU

A proteção de dados pessoais está inserida sob a responsabilidade do Diretor(a) Jurídico(a) de cada BU, que indica, quando apropriado, um Gestor de Proteção de Dados (GPD). Ou então, o(a) próprio(a) Diretor(a) Jurídico(a) será o GPD da BU. O GPD coordena as atividades relacionadas à proteção de dados pessoais na BU e será o ponto primário de contato com o Gestor de Proteção de Dados do Grupo.

As missões do GPD da BU estão listadas no Apêndice 2.

Se for apropriado, as BUs podem também decidir indicar um GPD em qualquer de suas Entidades envolvidas com Processamento de Dados (Clientes, RH, etc.)

Todos GPDs devem ter os recursos e o tempo necessários para realizar as missões a eles designadas. Cada GPD deve ser indicado oficialmente pela Direção de sua BU ou Entidade e deve receber uma carta de missão.

Para realizar suas obrigações, os GPDs das BUs e Entidades devem solicitar apoio dos Correspondentes de Proteção de Dados (CPDs) identificados no seu perímetro (divisões, departamentos, etc.).

3.3. A nível de Entidade

Cada Entidade é responsável pelo Processamento de Dados que ela implementa (ou que tenha sido implementado por um Processador de Dados) e o Representante Legal da Entidade será responsável por garantir a conformidade com as leis de Proteção de Dados aplicáveis àquela Entidade.

As missões do GPD da Entidade estão listadas no Apêndice 2.

Cada Entidade garantirá a conformidade com a Política de Privacidade de Dados do Grupo e com as leis de Proteção de Dados aplicáveis antes da implementação do Processamento de Dados, bem como durante sua execução e operação.

Se a lei assim o exigir, um GPD (ou qualquer pessoa expressamente indicada para esta finalidade) será indicado para garantir a conformidade com a legislação local, a qual pode por exemplo estipular que a Autoridade de Proteção de Dados seja notificado sobre qualquer Processamento de Dados.

3.4. Relativamente às BUs e Entidades na União Europeia

Conforme o regulamento Europeu sobre proteção de dados pessoais, ao ser nomeado, o GPD da BU e/ou Entidade deve garantir conformidade com a legislação.

As obrigações específicas do GPD, conforme o Regulamento Europeu, se encontram descritas no Anexo 2.

Os GPDs devem receber os recursos e ter o tempo necessário para realizar as missões designadas. Uma vez que são responsáveis pela aplicação desta Política em conformidade com o Regulamento Europeu, os GPDs devem estar aptos para se reportarem ao Comitê Executivo da BU ou Entidade.

Por conta da especialidade exigida pelos GPDs, é recomendado que as BUs ou Entidades localizadas em um mesmo país com um número limitado de Processamento de Dados, indiquem um GPD compartilhado.

Em alguns casos, é concebível que diversas BUs em um único país possam compartilhar o mesmo GPD.

De acordo com o Regulamento Europeu, cabe à BU ou, se aplicável, a cada Entidade decidir com a ajuda do Gestor de Proteção de Dados do Grupo, se o GPD necessita ser designado para a Autoridade Supervisora.[4] Assim sendo, ele/ela se tornará Diretor de Proteção de Dados (DPD) como definido no Regulamento Geral de Proteção de Dados.

Se a BU ou Entidade decidir designar o GPD à Autoridade Supervisora, o GDP deve ser:
- Sujeito às exigências de sigilo profissional e deve ter acesso direto aos dados (isto significa que o acesso aos dados não será negado aos GPDs);
- Independente e se reportar ao nível mais elevado da organização (deve ser elaborada uma declaração de missão específica e procuração);
- Obrigado a notificar a Autoridade Supervisora sobre quaisquer incidentes (violação de dados) dentro de 72 horas, e se for necessário, informar os Sujeitos dos Dados;
- Exigido que conduza (ou providenciar a realização de) auditorias e verificações.

O Gestor de Proteção de Dados do Grupo é também GPD do NewCorp e será designado à Autoridade Supervisora da França (CNIL), como DPD para (isto é, da ENGIE S.A.) Processamento de Dados que são transversais às Entidades Europeias.

3.5. *Stakeholders* – outras partes interessadas

Os Diretores de Segurança Cibernética e Informação (DSCI) oferecerão seu apoio e especialidade na área de Privacidade de Dados, tanto para os fins de processamento de dados hospedados internamente como junto a terceiros. As funções básicas dos DSCIs nesta área são as seguintes:
- Apoiar os GPDs/DPDs na classificação de Dados Pessoais (ver Política do Grupo sobre Proteção de Bens) e na implementação do gerenciamento de projeto de Segurança de Informação (ver § processo de risco “A

[4] Em alguns casos isto pode ser obrigatório, como indicado pelos Regulamentos Europeus.

montante").
- Aconselhar na seleção de funções e sistemas de Privacidade de Dados.
- Ser o ponto de contato para todas as solicitações relacionadas a aspectos de confidencialidade e segurança para um Processamento de Dados em execução.

Os Gerentes de Projeto agem em nome do Controlador de Dados e gerenciarão os projetos que implicam no processamento de Dados Pessoais. Eles devem garantir que a Privacidade de Dados seja mantida no decorrer do projeto.

Os Departamentos Jurídicos e de Recursos Humanos oferecerão aconselhamento e informação com relação a legislação e jurisprudência aplicáveis.

Os Diretores/correspondentes de Ética aconselharão o Gestor de Proteção de Dados do Grupo e o respectivo GPD/DPD com relação a incidentes registrados em INFORM'ethics.

Todos os funcionários (tanto temporários como permanentes) são responsáveis, pelos Dados Pessoais que eles acessam e processam.

Todo o pessoal que esteja implementando uma aplicação ou aplicativo que processa Dados Pessoais deve primeiro informar o GPD/DPD da BU/Entidade, uma vez que Processamento de Dados pode exigir uma notificação prévia à Autoridade de Proteção de Dados.

Qualquer terceiro prestando serviços, incluindo Processamento de Dados, em nome de uma Entidade deve estar ciente dos princípios desta Política com respeito a Dados Pessoais que eles acessem e processem.

4. Os princípios de Proteção de Dados

Os princípios de proteção apresentados abaixo aplicam-se a todas as BUs e Entidades, salvo se a legislação nacional dispuser em contrário ou for mais rigorosa.

4.1. Finalidades explícitas, legítimas, justas e transparentes

Dados Pessoais devem ser coletados e processados por meios justos para fins específicos, explícitos e legalmente previstos e não devem ser usados ou processados subsequentemente de uma forma incompatível com estas finalidades.

Conformidade com estes princípios de legalidade e justiça podem exigir[5], sob certas legislações de Proteção de Dados:
- Que o Sujeito dos Dados seja informado do Processamento de Dados e as finalidades;
- Que o Sujeito dos Dados dê o seu consentimento expresso ao Processamento de Dados; e/ou
- Que a Autoridade de Proteção de Dados local seja notificada sobre o Processamento de Dados.

Dados Pessoais podem ser comunicados entre serviços, departamentos, para outras Entidades do Grupo ou a terceiros somente em relação às finalidades do Processamento de Dados. Os Sujeitos dos Dados devem ser informados (ou às vezes consentir com) esta comunicação de seus Dados Pessoais.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu

Dentro da União Europeia, qualquer informação enviada ao Sujeito dos Dados relacionada com o processamento de seus dados deve ser concisa, facilmente acessível e de fácil compreensão, com elementos visuais quando apropriado.

Todas as transferências subsequentes devem ser objeto de uma notificação de processamento de dados de quando o consentimento foi dado.

BUs e Entidades na AEE ou BUs e Entidades fornecendo produtos na AEE devem ser capazes de fornecer

[5] GPD responsável por verificar o que é exigido pela legislação de proteção de dados aplicável.

prova à Autoridade Supervisora do consentimento do Sujeito dos Dados para o processamento (quando o consentimento é usado como motivo legalmente previsto para o processamento de dados).

4.2. Relevância, minimização e proporcionalidade dos dados coletados

Os Dados Pessoais coletados devem ser apropriados, relevantes e não excessivos com relação à finalidade para a qual são coletados e seu subsequente processamento. Devem ser precisos, abrangentes e atualizados se necessário.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:

Dentro da União Europeia, sob o princípio da minimização, os dados coletados devem ser adequados, relevantes e limitados ao que é estritamente necessário que estes sejam processados.

4.3 Um período limitado de retenção/arquivamento

O período de retenção dos Dados Pessoais processados deve ser definido de acordo com a finalidade da coleta e atendendo às leis aplicáveis. Uma vez que os Dados Pessoais não sejam mais necessários para a finalidade que legitimou seu processamento, eles devem ser excluídos ou tornados anônimos.

Portanto é aconselhável organizar a exclusão automática ou manual dos dados baseado em períodos de retenção pré-determinados.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:

Sujeitos de Dados devem ser notificados do período de retenção quando forem informados do Processamento dos Dados, ou, se isto não for possível, que o critério usado para determinar aquele período de retenção seja comunicado.

4.4 Dados Sensíveis, arquivos sensíveis e processamento em risco

Alguns Dados Pessoais são considerados sensíveis. Estes dados envolvem a esfera íntima dos Sujeitos dos Dados ou podem dar margem, no caso de mau uso, a discriminação ilegal ou arbitrária.

Particularmente, Dados Pessoais versando, especialmente, sobre origem racial ou étnica, opiniões ou crenças religiosas ou filosóficas ou relacionadas à saúde da pessoa ou vida sexual devem ser considerados sensíveis.

Adicionalmente, é necessário verificar as leis de Privacidade de Dados aplicáveis à Entidade, para identificar qualquer outro Dado Pessoal considerado sensível e estar em conformidade com exigências específicas relacionadas a Dados sensíveis de acordo com as leis aplicáveis.

Deve ser dada atenção especial ao Processamento de Dados Sensíveis:
O Controlador de Dados só pode processar Dados Sensíveis com o consentimento explícito do Sujeito dos Dados sob circunstâncias limitadas expressamente autorizadas por legislação nacional e/ou legislação Europeia.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:

Dados Sensíveis (chamados “categorias especiais de dados” no regulamento Europeu) também incluem: filiação a sindicato e o processamento de dados genéticos ou biométricos para a identificação única de um indivíduo.

Além disso, os seguintes são considerados “Processamento de Risco”, exigindo cuidado especial:
- Processamento que venha a excluir um indivíduo de gozar um direito, benefício ou contrato;
- Processamento envolvendo a interconexão de arquivos que tenham finalidades diferentes;
- Processamento envolvendo a transferência de Dados Pessoais para fora da União Europeia.

4.5 Obrigações de Confidencialidade e Segurança

Todas as medidas apropriadas de proteção devem ser tomadas com relação à natureza dos dados e os riscos apresentados pelo Processamento de Dados para garantir que os Dados Pessoais estejam seguros e mantidos confidenciais, particularmente, para protege-los de serem distorcidos ou danificados, bem como impedir o acesso não autorizado aos dados.

Estas medidas dependerão do risco existente, das possíveis consequências para o Sujeito dos Dados, da sensibilidade dos Dados Pessoais, da tecnologia disponível e da prática geral aceita nas jurisdições relevantes à Entidade.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:

Para garantir a segurança e a confidencialidade dos Dados processados, devem ser tomadas medidas tais como Pseudonimização, Anonimização e Criptografia.

4.5.1 Classificação e Proteção de Dados Pessoais

Como regra geral, Dados Pessoais são classificados como “Interno” ou “Restrito” (conforme a Política de Ativos do Grupo).

Da mesma forma, Dados Sensíveis são classificados como “Restrito” ou “Secreto”.

A classificação de Dados Pessoais deverá ser identificada na etapa de Privacidade por Design.
Dados Pessoais devem ser protegidos de acordo com as políticas da ENGIE e padrões de segurança relacionados à Segurança Cibernética e da Informação.

4.5.2 Processo de risco “*upstream*”

A implementação de novas atividades de Processamento de Dados deve ser acompanhada pelas seguintes ações durante as diferentes fases do projeto:

- Privacidade por Padrão: está relacionado primariamente com os princípios de limitação e minimização de dados (os dados coletados são estritamente necessários para a finalidade do Processamento de Dados), armazenagem de dados (relacionado à finalidade do Processamento de Dados), e Anonimização.

- Privacidade por Design: isto exige que o sistema e as soluções de tecnologia incorporem Proteção de Dados no estágio mais inicial possível de sua criação e desenvolvimento.

- Avaliação de Impacto da Privacidade: isto determina o nível de risco para os Sujeitos dos Dados (isto é, no evento de perda ou comprometimento de seus Dados) e para a Entidade (no evento de prejudicar sua imagem ou sua reputação) e tem como objetivo identificar as medidas de proteção adequadas.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:

Análise de impacto deve ser realizada ou supervisionada pelo GPD/DPD. Qualquer análise que exponha um risco a um Sujeito de Dados que não possa ser resolvida deve ser submetido à Autoridade Supervisora para consulta.

4.6 Transferências Internacionais

Quando as BUs e Entidades (fora da AEE) transferem Dados Pessoais para outras Entidades ou terceiros (também fora da AEE), elas devem garantir que os países para os quais os dados são transferidos, oferecem um nível mínimo de proteção descrito na política atual (exceto exigências específicas da UE).

Leis e regulamentos existentes definirão as condições das transferências internacionais e, quando necessário, cláusulas contratuais apropriadas deverão ser incluídas nos contratos entre os remetentes (os "exportadores") e os destinatários (os "importadores") de tais Dados Pessoais, para garantir um nível adequado de proteção dos Dados Pessoais.

A Entidade envolvida em transferência de dados com o Grupo se empenha para assinar e implementar as Regras Corporativas Vinculativas (BCR) da ENGIE.

Transferências internacionais de Dados Pessoais pelas BUs e Entidades europeias para países fora da UE não se beneficiam de uma decisão de adequação pela Comissão Europeia e, portanto, devem ser realizadas sob a égide das RCV aprovadas pelas Autoridades de Proteção de Dados ou por todos os meios disponibilizados pelas autoridades europeias.

4.7 Abertura e respeito pelos direitos individuais

Os Sujeitos de Dados têm o direito de controlar a informação relacionada a eles (seus Dados Pessoais). Eles serão informados de qualquer Processamento de Dados dos seus Dados Pessoais previamente à efetiva implementação do Processamento de Dados. Além disso, eles possuem o benefício, do direito de acesso e de retificação de seus Dados Pessoais, a qualquer tempo.

Os Sujeitos de Dados também têm o direito de se opor qualquer momento ao processamento de seus Dados Pessoais mediante evidência suficiente relacionada a sua situação pessoal específica, mesmo que o Sujeito de Dados tenha lhe dado consentimento específico para este processamento.

Serão implementadas políticas transparentes com relação a Processamento de Dados. Portanto, será fornecida informação básica aos Sujeitos de Dados com respeito à identidade dos Controladores de Dados e a forma como os Sujeitos de Dados podem exercer seus direitos de acesso, retificação e/ou exigência de exclusão ou encerramento do processamento de seus Dados Pessoais.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:

Adicionalmente aos direitos acima mencionados, os Sujeitos de Dados podem:
- Solicitar uma restrição no Processamento de seus Dados;
- Opor-se ao Processamento de seus dados, especificamente quando automatizado para fins de perfil.

Estes Direitos podem ser exercidos a qualquer momento, mesmo se os Sujeitos de Dados deram seu consentimento expresso ao Processamento de Dados, ou eles podem solicitar que os últimos sejam limitados.

O Regulamento Europeu fortaleceu e também impôs novos direitos entre os quais:

- A informação relacionada aos Sujeitos dos Dados é reforçada e precisa incluir o seguinte:
  - O período de retenção deve ser indicado;
  - O direito de enviar uma reclamação à Autoridade Supervisora deve ser explicado;
  - Qualquer decisão de usar dados para subsequente processamento para fins diferentes daqueles que aqueles para os quais os Dados Pessoais foram coletados deve ser indicada;
  - Qualquer uso de informação para fins de criação de perfil;
  - Origem dos Dados, se não foram coletados diretamente dos Sujeitos dos Dados.
  - ...
- O consentimento deve ser um ato afirmativo claro, estabelecendo uma indicação dada livremente, específica, informada e não ambígua da concordância dos Sujeitos dos Dados ao processamento de seus Dados Pessoais tal como uma declaração por escrito, incluindo por meios eletrônicos ou uma declaração oral e deve ser clara, explícita e inequívoca. A prova do consentimento deve ser conservada de qualquer forma. Este consentimento pode ser retirado a qualquer tempo.
- O direito à portabilidade de dados significa que os Sujeitos dos Dados podem obter de volta o controle de seus Dados Pessoais e se beneficiar do uso de seus Dados Pessoais. O Controlador de Dados deve devolver

seus dados a eles em um formato acessível e legível. Os Sujeitos dos Dados podem solicitar que seus Dados Pessoais sejam diretamente transferidos a um terceiro.

- O Regulamento Europeu possibilita que os Sujeitos de Dados façam uso do seu 'direito de ser esquecido' a qualquer tempo, inclusive especialmente quando a retenção de dados constitui uma violação deste regulamento. Isto inclui o direito de ter seus dados excluídos e não mais processados quando não são mais necessários para as finalidades que embasaram a sua coleta.

4.8 Obrigações dos Processadores de Dados

Qualquer Entidade que subcontrate um Processamento de Dados a um Processador de Dados, permanece responsável pela proteção dos Dados Pessoais. As Entidades devem garantir que estas partes processem os dados conforme os princípios da Política de Proteção à Privacidade de Dados do Grupo.

Processadores de Dados serão selecionados por sua capacidade de oferecer garantias com relação à proteção de Dados Pessoais. Um contrato ou acordo escrito deve ser estabelecido prevendo as obrigações do Processador de Dados para cumprir com as regras de proteção de Dados Pessoais incluindo medidas de confidencialidade e segurança.

5 Os meios de Proteção de Dados

Os seguintes meios devem ser implementados pelas BUs e Entidades para atingir os objetivos desta Política.

5.1 Conscientização e Treinamento

Todo pessoal das BUs e Entidades deve ser conscientizado acerca dos temas envolvendo Privacidade de Dados. Campanhas de conscientização global são conduzidas a nível de Grupo; as campanhas são delegadas aos Gestores de Proteção de Dados (GPDs) para ser distribuídas a todos os empregados das Entidades. Ações locais devem ser efetuadas pelas BUs e Entidades para complementar estas campanhas.

Treinamento básico dos GPDs e Correspondentes de Privacidade de Dados (CPDs) é fornecido pelo Grupo de Gestores de Privacidade de Dados. GPDs e CPDs das BUs e Entidades devem atender a treinamentos adicionais para adquirir a capacitação necessária para cumprir com suas tarefas.

5.2 Revisões e Auditorias

Revisões internas para conformidade com esta Política e as leis de Proteção de Dados devem ser feitas regularmente pelo Representante Legal da BU ou Entidade que delegará esta atividade ao seu GPD e DSCI O Gestor de Privacidade de Dados do Grupo pode também proceder com estas revisões.

Como parte destas revisões, o acesso aos processos e Dados, assim como, por exemplo, as medidas de confidencialidade e segurança e períodos de retenção devem ser avaliadas e controladas.

A condução efetiva destas ações pode estar sujeita a auditorias conduzidas pelo Departamento de Auditoria Interna.

5.3 Mapeamento do Processamento de Dados

Com relação ao princípio da Acessibilidade, para facilitar o exercício do direito de acesso dos Sujeitos de Dados, é recomendado que cada Entidade estabeleça um mapa e um registro[6] de todo Processamento de Dados significativo. Este mapa permitirá uma visão geral, assim como possibilitará que o Processamento de Dados seja controlado e racionalizado e o registro facilitará que o Controlador de Dados lide com uma

[6] Para BUs e Entidades relacionadas com o Regulamento Europeu, o registro é uma obrigação.

solicitação de acesso do Sujeito de Dados.

5.4 Lidando com Incidentes

Qualquer pessoa que saiba de um uso inapropriado de Dado Pessoal irá contatar seu GPD/DPD, que reportará o incidente ao Diretor de Ética, sendo este último responsável por reportar este incidente no INFORM'ethics. O Departamento de Ética & Conformidade informará o Gestor de Proteção de Dados do Grupo sobre qualquer incidente reportado no INFORM'ethics.

Assim que estiver claro que um incidente tem um impacto potencial na Privacidade de Dados, o Gestor de Proteção de Dados do Grupo deverá ser informado e lidará com a situação em colaboração com os outros membros do Comitê de Tratamento de Incidentes (juntamente com a Entidade envolvida).

No caso em que seja necessário gerenciamento de crise para lidar com o incidente, o Gestor de Proteção de Dados do Grupo será um dos membros designados do centro de crise para a resolução do incidente.

Exigências específicas para BUs e Entidades sujeitas ao Regulamento Europeu:
Os GPDs/DPDs de BUs e Entidades terão que notificar violações de dados dentro de 72 horas à sua Autoridade Supervisora e, quando necessário, aos Sujeitos de Dados afetados.

5.5 Contratos Escritos

Nos casos de aquisição, uso ou subcontratação de Dados Pessoais (por exemplo, para o fornecimento de ofertas adicionais para clientes e possíveis clientes da ENGIE) um contrato escrito deve ser estabelecido entre as partes em questão (ENGIE, seus clientes ou parceiros). Em qualquer circunstância, a coleta, uso ou subcontratação de Dados Pessoais deve estar de acordo com as leis vigentes, o Código de Ética da ENGIE e esta Política.

6 Sistema de Gerenciamento e Responsabilidade

6.1 Sistema de Gerenciamento de Proteção de Dados

Para acompanhar as BUs e garantir um gerenciamento de Proteção de Dados eficiente e em contínua melhora, um Sistema de Gerenciamento foi estabelecido e colocado sob a supervisão do Comitê de Privacidade. O escopo do Sistema de Gerenciamento é a totalidade do Grupo.

O Sistema de Gerenciamento consiste em atividades múltiplas destinadas a medir a conformidade pela NewCorp e as BUs com a Política e a legislação. Estas atividades incluem aquelas relacionadas com:

- A implementação da governança;
- O desenvolvimento de elevação da conscientização e sessões de treinamento;
- A conformidade do Processamento com a legislação;
- A administração de violação de Dados.

Estas atividades estão formalizadas dentro da estrutura de procedimentos e documentos acompanhando a implementação da Política.

6.2 Prestação de Contas (exigência específica do Regulamento Europeu)

Prestação de Contas ou responsabilização é o princípio fundamental do Regulamento Europeu. Ela envolve responsabilidades atribuídas ao Controlador de Dados.

O Controlador de Dados deve ser capaz de demonstrar a todo o tempo que está em conformidade com os princípios relacionados ao processamento de Dados Pessoais.

Em essência, ele deve implementar todas as medidas apropriadas e efetivas, e estar em condições de demonstrar que o Processamento de Dados está conforme, bem como a efetividade das medidas tomadas.

A Prestação de Contas também resulta na implementação de um registro de Processamento de Dados (e seu gerenciamento apropriado ao longo do tempo), a implementação de procedimentos tais como

Privacidade por Design, Privacidade por Padrão, Avaliação de Impacto da Privacidade, e colocando etiquetas, distintivos, certificações e códigos de conduta em relação à Proteção de Dados.

A implementação desta Política é um dos componentes essenciais da Prestação de Contas para atingir a conformidade com o Regulamento Europeu.

Apêndice 1: Definições

“Anonimização ”: qualquer informação relacionada a uma pessoa física onde a pessoa não possa ser identificada, seja pelo Controlador de Dados ou por qualquer outra pessoa, levando em conta todos os meios possivelmente razoáveis a serem usados seja pelo Controlador ou qualquer outra pessoa para identificar aquela pessoa.

" Área Econômica Europeia (AEE) ": é a área na qual o Acordo sobre a AEE dispõe movimento livre de pessoas, mercadorias, serviços e capital no âmbito do mercado interno da União Europeia (UE).

“Autoridade de Proteção de Dados": Autoridade ou instituição responsável pelo cumprimento e monitoramento da conformidade com a legislação de proteção de dados a nível nacional. Ver também **Autoridade Supervisora**.

“Autoridade Supervisora“: uma autoridade pública independente que seja estabelecida por um Estado Membro para ser responsável por monitorar a aplicação deste Regulamento, para proteger os direitos fundamentais e liberdades das pessoas físicas com relação ao processamento e por facilitar o fluxo livre de Dados Pessoais no âmbito da União Europeia.

“Big Data”: Big Data refere-se a conjuntos de dados de volume extremamente grande que são difíceis de trabalhar usando gerenciamento de base de dados ou ferramentas de gerenciamento da informação tradicionais. As expectativas de processamento de dados de Big Data são enormes, particularmente para análise de opiniões políticas, tendências industriais, combate ao crime, etc.

"**Código de Ética**": O Código de Ética define os princípios de ética que cada funcionário do Grupo deve praticar quando exercendo seus deveres profissionais e em seus comportamentos perante todos contatos no âmbito do Grupo.

“Comitê de Tratamento de Incidentes”: com a presidência do Diretor de Segurança, o Comitê de Tratamento de Incidentes compreende representantes do departamento de Saúde e Segurança, do Departamento de RH, do Departamento Jurídico, do Departamento de SI e representantes da Entidade envolvida no incidente. O Comitê qualifica o impacto potencial a nível de Grupo e age como um coordenador lidando com o incidente de segurança.

"Controlador de Dados": a pessoa física ou jurídica responsável por determinar a finalidade e métodos de Processamento de Dados que foram implementados ou devem ser implementados. O Controlador de Dados é obrigado a tomar todas as precauções necessárias para garantir a Privacidade de Dados.

"Correspondente de Proteção de Dados (CPD) ": Este é o intermediário do GPD/DPD com relação à proteção de Dados Pessoais no âmbito dos departamentos das BUs ou Entidades.

" Criptografia ": é o processo de codificar mensagens ou informação de tal forma que somente partes

autorizadas possam lê-la.

"Dados Pessoais": qualquer informação relacionada a uma pessoa, como uma pessoa física (**"Sujeito de Dados"**), identificada ou capaz de ser identificada, direta ou indiretamente, ao referir-se a um número de identificação ou a um ou mais elementos específicos a ele/ela (por exemplo sobrenome, primeiro nome, CPF, endereço de e-mail, endereço de IP, etc.).

"Dados Sensíveis": Dados Pessoais que podem afetar a esfera íntima do Sujeito de Dados ou que em caso de mau uso, possam dar origem a discriminação (por exemplo origem racial ou étnica, opinião política, crença religiosa ou filosófica, dados relacionados a sua saúde ou vida sexual, etc.,).

"**Diretor de Proteção de Dados" (DPD)**: Na União Europeia, o Diretor de Proteção de Dados é a pessoa designada de acordo com as disposições obrigatórias da GDPR perante sua Autoridade Supervisora.

"DSCI ou Diretor de Segurança Cibernética e de Informação (CISO em Inglês) ": o gerente encarregado em cada BU da efetivação da Política de Segurança Cibernética do Grupo para suas Entidades reportando funcionalmente ao Diretor de Segurança Cibernética e Informação do Grupo.

" Entidade ": pessoa jurídica no âmbito do escopo consolidado do Grupo (integração global).

"Gerente de Projeto": uma pessoa física atuando em nome do Controlador de Dados, que gerencia o projeto até que o Processamento de Dados tenha sido implementado. O Gerente de Projeto deve garantir que a Privacidade de Dados seja mantida e respeitada ao longo de todo o projeto.

"Gestor de Privacidade de Dados" (**GPD**): A pessoa designada no âmbito da BU ou Entidade como responsável pelas ações relacionadas à proteção de Dados Pessoais. Quando indicado para esta função, ele/ela recebe uma carta de nomeação e procuração (quando necessário) de seus superiores hierárquicos.

"Grupo": Grupo ENGIE.

" NewCorp ": organização que compreende os Métiers, as Funções Operacionais e as Funções de Suporte.

"NUVEM (ou Computação na Nuvem)**"**: Computação na nuvem significa acesso a recursos de TI compartilhados configuráveis via uma rede de telecomunicações, em uma base on demand e self-service.

"Privacidade de Dados"/ "Proteção de Dados": conjunto de **ações, atividades, métodos, processos**, organizações e assim por diante com o objetivo de proteger Dados Pessoais e de garantir conformidade com as leis e regulamentos aplicáveis a Privacidade de Dados.

"Processador de Dados": subcontratado a quem o Controlador de Dados designa toda ou parte das operações relacionadas a seu Processamento de Dados, tais como a implementação, a hospedagem, a operação, o gerenciamento, etc.

"Processamento de Dados": qualquer operação ou conjunto de operações envolvendo Dados Pessoais, por qualquer método ou meio usado (Processamento automático de Dados tais como aplicações de TI,

arquivos de dados Excel, etc., ou Processamento de Dados não automático incluído ou com a intenção de ser incluído em um sistema de arquivo estruturado por meio do qual Dados Pessoais estão acessíveis conforme um critério específico como, por exemplo, arquivos individuais de funcionários, etc.), particularmente a coleta, registro, organização, armazenagem, adaptação ou alteração, recuperação, consulta, uso, disponibilização por transmissão, disseminação ou outra forma de circulação, alinhamento ou consolidação, bloqueio, exclusão ou destruição.

"Pseudonimização": é a separação de dados de identificadores diretos de forma que a conexão a uma identidade não seja possível sem informação adicional que é mantida em separado. A pseudonimização, portanto, pode reduzir significativamente os riscos associados com Processamento de Dados, ao mesmo tempo mantendo a utilidade dos dados.

"Regras Corporativas Vinculativas ou BCR": devem suplementar a Política de Privacidade de Dados do Grupo e o Código de Ética para garantir um nível adequado de proteção para as transferências e Processamento de Dados relacionados dos Dados Pessoais dos Sujeitos de Dados dentro do Grupo ENGIE e facilitar transferências em todo o Grupo, em conformidade com as exigências legais aplicáveis, particularmente aqueles estabelecidos tanto na Diretriz UE 95/46 datada de 24 de outubro de 1995 sobre proteção de pessoas com relação ao processamento de Dados Pessoais e sobre o livre movimento de tais dados, e a Diretriz UE 02/58/EC datada de 12 de julho de 2002 e alterações, relativa ao processamento de Dados Pessoais e à proteção de privacidade no setor de comunicações eletrônicas.

" Regulamento Europeu " ou "GPDR": (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção das pessoas físicas em relação ao processamento de Dados Pessoais e sobre o livre movimento de tais dados, e revogando a Diretriz 95/46/EC (RGPD – Regulamento Geral de Proteção de Dados). Entra em vigor em 25 de maio de 2018.

"Sistema de Gerenciamento de Privacidade de Dados": é a estrutura de atividades, processos e procedimentos de Proteção de Dados pelos quais o Grupo efetiva o cumprimento da Política de Privacidade de Dados do Grupo.

"**Sistema de Informação (SI)":** grupos estruturados de processos e recursos organizacionais, materiais e de software que tornam possível adquirir, processar, armazenar, distribuir e destruir a informação em formato eletrônico.

"Sujeito de Dados": uma pessoa física cujos Dados Pessoais estão sendo processados por um Controlador de Dados ou um Processador de Dados.
"BU ou Business Unit": Unidade de Negócios, corresponde ao agrupamento de Entidades. BUs não tem status jurídico.

Apêndice 2: As missões do DPD de Grupo e dos GPDs das BUs e Entidades

1 - Missões do Diretor de Proteção de Dados (DPD) do Grupo

Os principais deveres do Diretor de Proteção de Dados do Grupo são os seguintes:

- Garantir a implementação efetiva da Política de Privacidade de Dados do Grupo e monitorar sua aplicação.
- Definir e disseminar as boas práticas com relação ao uso de Dados Pessoais (clientes, funcionários, fornecedores, etc.,) juntamente com as BUs e Entidades
- Garantir que elas sejam implementadas, bem como alertar os gerentes e aconselhá-los sobre quaisquer riscos associados.
- Liderar a rede de **Gestores de Proteção de Dados** (**GPDs**), conforme definido pelas BU's, por meio do Comitê de Privacidade de Dados.
- Representar o Grupo nesta área perante os agentes externos e atores para tópicos transversais.
- Monitorar os desenvolvimentos dos regulamentos nos principais países onde o Grupo está ativo.
- Coordenar o gerenciamento dos incidentes de Privacidade de Dados que impactem o Grupo com os GPDs envolvidos.
- Implementar o Sistema de Gerenciamento de Privacidade de Dados.

2 - Missões de GPDs a nível de cada BU

Os principais deveres dos GPDs da BU são os seguintes:

- Garantir a implementação efetiva desta Política (ou sua versão customizada para a BU) e monitorar sua aplicação.
- Garantir que os regulamentos aplicáveis à proteção de Dados Pessoais sejam levados em consideração no âmbito da BU.
- Participar em campanhas de conscientização voltadas ao pessoal da BU.
- Participar nas atividades organizadas pelo Diretor de Proteção de Dados do Grupo (boas práticas, feedbacks, etc.,) e ser um membro ativo da rede.
- Informar o DPD do Grupo dos GPDs/DPDs identificados a nível de Entidade.
- Gerenciar a rede de GPDs/DPDs e os Correspondentes de Proteção de Dados (CPDs) no âmbito da BU conforme necessário.
- Efetuar um relatório anual das atividades de Proteção de Dados e comunica-lo ao Diretor de Proteção de Dados do Grupo.
- Informar o Diretor de Ética local e o Diretor de Proteção de Dados do Grupo de qualquer uso inapropriado de Dados Pessoais ou quaisquer incidentes que os envolvam

Caso o GPD da BU não identifique GPDs para as Entidades, ele será responsável pelas missões deles assim como da dele próprio.

3 - Missões de GPDs a nível de Entidade

Os principais deveres dos GPDs da Entidade são os seguintes:

- Garantir a implementação efetiva desta Política (ou sua versão customizada para a Entidade) e monitorar sua aplicação.
- Garantir que os regulamentos aplicáveis à proteção de Dados Pessoais sejam respeitados no âmbito da Entidade.
- Apoiar o esforço da conformidade do Processamento de Dados e conduzir as formalidades junto às Autoridades de Proteção de Dados quando necessário.
- Informar e aconselhar os Controladores de Dados sobre as questões de Privacidade de Dados e se

necessário, chamar sua atenção para estas questões.
- Participar em campanhas de conscientização voltadas ao pessoal da Entidade.
- Participar nas atividades organizadas pelo Gestor de Proteção de Dados da BU (boas práticas, feedbacks, etc.,) e ser um membro ativo da rede.
- Efetuar um relatório anual das atividades de Proteção de Dados da Entidade e comunica-lo ao GPD da BU.
- Informar o Diretor de Ética local e o GPD da BU de qualquer uso inapropriado de Dados Pessoais ou quaisquer incidentes que os envolvam.

- **Deveres adicionais e específicos dos GPDs das BU's e Entidade na Europa:**
- Participar nas avaliações de impacto na privacidade;
- Garantir responsabilização, prestação de contas;
- Implementar e manter o registro do Processamento de Dados;
- Expedir notificações sobre quaisquer violações de dados à Autoridade Supervisora.

As missões dos Correspondentes de Proteção de Dados (CPDs) a quem os GPDs de BU e Entidade venham a chamar para apoio incluirá a promoção desta Política, comunicando ao GPDs sobre situações de Processamento de Dados que exijam atenção específica, participando da rede de GPDs, ...

Apêndice 3: Documentos de Referência sobre Proteção de Dados

Acesso à Declaração Universal de Direitos Humanos : http://www.un.org/en/documents/udhr/

O Artigo 12 da Declaração Universal de Direitos Humanos das Nações Unidas declara: *Ninguém será sujeito à interferência arbitrária de sua privacidade...* Artigo 17 da Convenção Internacional dos Direitos Civis e Políticos (Gabinete do Alto Comissariado para os Direitos Humanos) declara: *Ninguém será sujeito à interferência ilegal ou arbitrária de sua privacidade.*

Acesso à Convenção Europeia dos Direitos Humanos : http://www.echr.coe.int/Documents/Convention ENG.pdf

Artigo 8 do Código de Direitos Fundamentais da União Europeia declara:

1. *Todos têm o direito à proteção de Dados Pessoais relativos a ele ou ela.*
2. *Tais dados devem ser processados justamente para fins específicos e com base no consentimento da pessoa a que se referem ou algum outro tipo de base legítima disposta por lei. Todos têm o direito de acesso a dados que tenham sido coletados relativos a ele ou ela, e o direito de tê-los retificados...*

Acesso à Convenção Internacional de Direitos Civis e Políticos: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Diretrizes da OCDE sobre Proteção da Privacidade e Fluxo de Dados Pessoais entre fronteiras (1980 / 2013)

Acesso às Diretrizes:
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Lista de membros (34 na data de publicação): http://www.oecd.org/about/membersandpartners/

Diretriz 95/46/EC sobre a proteção de pessoas com relação ao processamento de Dados Pessoais e sobre a livre movimentação de tais dados:

Acesso à Diretriz:
http://ec.europa.eu/justice/data-protection/index en.htm

Acesso aos Estados Membros (28 na data de publicação) : http://europa.eu/about-eu/countries/index en.htm

Regulamento da UE 2016/679 de 27/04/2016 sobre a proteção de pessoas físicas com relação ao processamento de Dados Pessoais e a livre movimentação de tais dados (aplicável a partir de 25 de maio de 2018):
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

APEC – Estrutura de Privacidade (2005)

Acesso à Estrutura de Privacidade:
http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx

Lista das Economias Membro da APEC : (21 na data de publicação) http://www.apec.org/about-us/about-apec/member-economies.aspx

GAPP/PPGA – Princípios de Privacidade Geralmente Aceitos – desenvolvidos pela AICPA & CICA (Agosto de 2009)

Acesso ao GAPP:
http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/pages/default.aspx

AICPA : American Institute of Certified Public Accountants / Instituto Americano de Contadores Públicos Registrados http://www.aicpa.org/Pages/default.aspx

CICA : Canadian Institute of Chartered Accountants / Instituto Canadense de Contadores Registrados

http://www.cica.ca/index.aspx

Resolução de Madri sobre uma Proposta Conjunta para um Esboço de Padrão Internacional sobre Proteção de Privacidade e Dados Pessoais (9/11/2009).

Acesso ao press release:
http://www.gov.im/lib/docs/odps/madridresolutionpressreleasenov0.pdf

Acesso ao Rascunho do Padrão Internacional / International Standard : http://www.gov.im/lib/docs/odps/madridresolutionnov09.pdf