SAUS, Quadra 6, Bloco E, 6º Andar, Ala Norte - Bairro Asa Sul, Brasília/DF, CEP 70070-940
Telefone: (61) 2312-2152 - https://www.gov.br/anatel

Importante: O Acesso Externo (www.anatel.gov.br/seiusuarioexterno) possibilita o Peticionamento Eletrônico para abrir Processo Novo, Intercorrente e Resposta de Intimação. Pesquisa Pública do SEI: www.anatel.gov.br/seipesquisa

Ofício nº 241/2026/PRRE/SPR-ANATEL

Ao Senhor

GUSTAVO JUNIOR ALVES

Campinas/SP

Assunto: **Esclarecimentos sobre obrigações de registro, retenção de dados e conformidade operacional em arquiteturas baseadas no *Participant Relationship Protocol* (PRP).**

Senhor Interessado,

1. Em atenção à Consulta Técnico-Regulatória à Anatel (SEI nº 16422323), apresentamos esclarecimentos sobre as obrigações de registro e conservação de dados na utilização do *Participant Relationship Protocol* (PRP). Essas obrigações decorrem do serviço prestado e da função exercida por cada agente. Assim, a adoção do protocolo não afasta os deveres aplicáveis à atividade, nem implica, por si só, a obrigação de conservar todas as informações disponíveis na rede.

2. Para delimitar os registros exigíveis, o art. 120 do Regulamento Geral dos Serviços de Telecomunicações (RGST), aprovado pela Resolução nº 777/2025, estabelece prazo mínimo de cinco anos para documentos fiscais e dados cadastrais. Esse prazo também se aplica, conforme o serviço, aos dados de bilhetagem e das ligações efetuadas e recebidas, incluindo data, horário, duração e valor. Já os registros de conexão à internet devem ser mantidos por, no mínimo, um ano. Cada prazo corresponde, portanto, a uma categoria de informação e não se estende indistintamente a todos os metadados operacionais.

RGST

> " Art. 120. A fim de assegurar a permanente fiscalização e o acompanhamento de obrigações legais e regulatórias, as prestadoras devem manter à disposição da Anatel os dados relativos à prestação do serviço, incluindo, conforme o caso e observada a regulamentação pertinente:
>
> I - documentos de natureza fiscal e dados cadastrais, pelo prazo mínimo de 5 (cinco) anos, para todos os serviços de telecomunicações;
>
> II - dados das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo mínimo de 5 (cinco) anos, nos serviços que permitam a realização de tráfego telefônico;
>
> III - dados de bilhetagem, pelo prazo mínimo de 5 (cinco) anos, nos serviços cabíveis; e,
>
> IV - registros de conexão à Internet pelo prazo mínimo de 1 (um) ano nos serviços que permitam a conexão à Internet.
>
> Parágrafo único. Para fins do disposto neste artigo, considera-se registro de conexão à Internet o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal, assim como as portas lógicas utilizadas quando do compartilhamento de IP público, para o envio e recebimento de pacotes de dados."

3. No caso da conexão à internet, os registros compreendem início, término, duração e endereço IP utilizado pelo terminal, incluindo portas lógicas quando houver compartilhamento de IP público, conforme o parágrafo único do art. 120 do RGST. O art. 13 da Lei nº 12.965/2014 (Marco Civil da

Internet) atribui a responsabilidade por essa guarda ao administrador do sistema autônomo respectivo, sob sigilo e em ambiente controlado e seguro, sem possibilidade de transferência da responsabilidade a terceiros. Complementarmente, o art. 15-A do Decreto nº 8.771/2016, incluído pelo Decreto nº 12.975/2026, exige a conservação da porta lógica de origem associada ao IP quando necessária à identificação inequívoca do terminal de origem ou do próximo enlace de rede. Essa obrigação independe de requisição prévia e recai autonomamente sobre cada provedor abrangido.

Lei nº 12.965/2014

> "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
>
> § 3º Na hipótese do § 2º , a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
>
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .
>
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência."

Decreto nº 8.771/2016

> "Art. 15-A. O dever de guarda de registros de endereço IP pelos provedores de conexão e pelos provedores de aplicações de internet, previsto nos art. 13 e art. 15 da Lei nº 12.965, de 23 de abril de 2014, abrangerá a porta lógica de origem associada sempre que necessário para a identificação inequívoca do terminal de origem ou do próximo enlace de rede. (Incluído pelo Decreto nº 12.975, de 2026)
>
> § 1º O dever de guarda da porta lógica de origem independerá de prévia requisição e recairá autonomamente sobre cada provedor. (Incluído pelo Decreto nº 12.975, de 2026)
>
> § 2º O fornecimento da porta lógica de origem e dos dados a ela vinculados observará o disposto nos art. 10 e art. 22 da Lei nº 12.965, de 23 de abril de 2014. (Incluído pelo Decreto nº 12.975, de 2026)"

4. Na aplicação dessas regras ao PRP, é necessário considerar o que cada identificador representa. Um endereço IP que corresponda a equipamento intermediário não identifica, por esse único fato, o participante final da comunicação. Essa distinção, porém, não dispensa o provedor dos registros relativos à conexão e ao usuário que atende, nem permite substituir IP e porta exigíveis por rótulos locais do protocolo. Para os trechos que não utilizem IP, o art. 15-A não estabelece identificador alternativo específico para o PRP, permanecendo aplicáveis as obrigações do serviço prestado.

5. Quanto aos demais elementos descritos na consulta, não se identifica norma específica que estabeleça campos obrigatórios de registro para o PRP. Informações sobre relações ou sessões adjacentes, horários, rótulos, volumes e meios de transporte devem ser conservadas quando integrarem registros exigidos, forem necessárias ao cumprimento de obrigação aplicável ou estiverem abrangidas por determinação competente. É o caso, por exemplo, de volumes utilizados no cálculo da cobrança, que podem integrar os dados de bilhetagem. Para facilitar a compreensão dos registros mantidos, recomenda-se documentar o significado dos identificadores, sua referência temporal e as associações pertinentes, sem que essa orientação institua formato obrigatório de registro.

6. A mesma lógica se aplica ao prestador de trânsito, que deve conservar os dados fiscais, cadastrais e de bilhetagem exigíveis em sua atividade e, se fornecer conexão à internet, os registros

correspondentes. Nesse contexto, cabe distinguir as informações presentes no protocolo daquelas decorrentes da relação com o usuário: o art. 119, inciso XIV, do RGST exige das prestadoras de interesse coletivo cadastro atualizado de seus usuários, observadas as exigências legais e as exceções regulamentares. Portanto, a ausência da identidade civil do participante nos campos do PRP não afasta o dever da prestadora de manter o cadastro dos usuários que atende diretamente.

RGST

> "Art. 119. Sem prejuízo do disposto na legislação aplicável e nos instrumentos de outorga e ressalvadas as exceções dispostas na regulamentação, as Prestadoras de serviços de telecomunicações de interesse coletivo têm a obrigação de:
>
> [...]
>
> XIV - manter cadastro atualizado de seus Usuários, inclusive se a divulgação do Código de Acesso foi autorizada, observadas as exigências legais;"

7. Em uma cadeia de prestadores independentes, a conservação distribuída pode ser compatível com a regulamentação, desde que cada agente cumpra suas obrigações e preserve a rastreabilidade exigível. O art. 29, inciso III, do Regulamento Geral de Interconexão (RGI), aprovado pela Resolução nº 693/2018, veda práticas que comprometam a rastreabilidade das conexões ou chamadas. Nesse sentido, os mecanismos de identificação e correlação adotados devem permitir o cumprimento das obrigações aplicáveis ao serviço, ainda que as informações estejam distribuídas entre diferentes prestadores. A ausência de uma chave global de correlação ponta a ponta não dispensa a produção e a conservação dos registros exigíveis, cuja suficiência deve ser avaliada à luz dessas obrigações.

RGI

> "Art. 29 São vedadas, no relacionamento de Interconexão, quaisquer práticas que:
>
> [...]
>
> III - comprometam a rastreabilidade das conexões e/ou chamadas;"

8. Essa avaliação deve considerar também eventuais funcionalidades de telefonia. Nos serviços que utilizem numeração pública conforme a Recomendação UIT-T E.164, o art. 136 do RGST exige identificação dos acessos, rastreabilidade das chamadas e garantia de manutenção ou suspensão do sigilo. Para o STFC e o SMP, o art. 2º do Despacho Decisório nº 978/2025/COGE/SCO determina o fornecimento à Anatel, quando solicitado, dos registros detalhados de chamadas e das rotas de tráfego. Embora essas exigências não se estendam automaticamente a todo tráfego PRP, devem ser observadas quando aplicáveis ao serviço. Por sua vez, o art. 134 do RGST prevê a disponibilização dos recursos necessários ao cumprimento de determinações de suspensão de sigilo, nos limites legalmente autorizados.

RGST

> "Art. 134. As prestadoras devem tornar disponíveis os recursos tecnológicos, facilidades e dados necessários à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes, e manter controle permanente de todos os casos, acompanhando a efetivação dessas determinações, e zelando para que elas sejam cumpridas, dentro dos estritos limites autorizados.
>
> § 1º Os equipamentos e programas necessários à suspensão do sigilo devem integrar a plataforma da prestadora, que deve arcar com os respectivos custos.
>
> § 2º Os demais custos operacionais relacionados a cada suspensão de sigilo poderão ter caráter oneroso para a autoridade demandante.
>
> § 3º A Anatel deve estabelecer as condições técnicas específicas para disponibilidade e uso dos recursos tecnológicos e demais facilidades referidas neste artigo, observadas as disposições constitucionais e legais que regem a matéria."
>
> "Art. 136. Constituem pressupostos essenciais à prestação de serviços de telecomunicações que fazem uso de numeração pública, conforme recomendação ITU-T E.164, a identificação do acesso individual ou coletivo de origem ou destino da chamada, a capacidade de rastrear a chamada e a garantia de manutenção ou suspensão do sigilo."

9. O cumprimento desses deveres deve ocorrer em conjunto com a proteção da privacidade. Os arts. 132 e 133 do RGST exigem sigilo, segurança e retenção limitada ao necessário, com exclusão dos dados quando atingida a finalidade do tratamento ou encerrado o prazo de guarda, respeitados os prazos obrigatórios e as hipóteses de preservação. Também é necessário distinguir quem fornece acesso à internet de quem oferece aplicações, como sites e aplicativos. Na provisão de conexão, o art. 14 do Marco Civil veda a guarda de registros sobre o uso dessas aplicações. Já o art. 15 exige que o provedor de aplicações constituído como pessoa jurídica e que exerça atividade organizada, profissional e econômica conserve, por seis meses, os registros de acesso à sua própria aplicação. Esses registros indicam quando e a partir de qual endereço IP ocorreu o acesso, sem se confundirem com o conteúdo de mensagens ou outras comunicações.

RGST

> Art. 132. As prestadoras devem zelar pelo sigilo das comunicações e pela confidencialidade dos dados dos usuários de seus serviços, inclusive registros de conexão, nos termos da legislação e regulamentação.
>
> Parágrafo único. As prestadoras devem utilizar os recursos tecnológicos necessários e disponíveis para assegurar a inviolabilidade do sigilo das comunicações, em especial, no caso do SMP e outros serviços que utilizem radiofrequências na rede de acesso, nos enlaces radioelétricos entre a Estação Rádio Base e a Estação Móvel.
>
> Art. 133. As prestadoras devem reter a menor quantidade possível de dados de usuários, mantendo-os sob sigilo e protegidos, em ambiente controlado e de segurança, excluindo-os:
>
> I - tão logo atingida a finalidade de seu tratamento; ou,
>
> II - quando encerrado o prazo de guarda determinado por obrigação legal ou regulatória.
>
> Parágrafo único. A guarda de dados de usuários deve observar o disposto no art. 120 inclusive quanto aos prazos.

Lei nº 12.965/2014

> "Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet."
>
> "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento."

10. Para assegurar sua proteção e utilização adequada, o armazenamento e o fornecimento dos dados devem observar os arts. 10, 13, 15 e 22 do Marco Civil e os arts. 11 e 13 a 15-A do Decreto nº 8.771/2016. Essas disposições abrangem segurança, controle e registro de acessos, formato interoperável e estruturado e preservação por prazo superior nas condições legais. O acesso a dados cadastrais por autoridade com competência legal expressa não autoriza acesso irrestrito aos registros de conexão. Da mesma forma, a necessidade de correlacionar informações de diferentes prestadores não permite compartilhamento indiscriminado nem transfere a responsabilidade de guarda.

Lei nº 12.965/2014

> "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham

competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais."

"Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º , a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º , que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º .

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência."

"Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência."

"Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros."

Decreto nº 8.771/2016

"Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014 , indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

§ 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.

§ 2º São considerados dados cadastrais:

I - a filiação;

II - o endereço; e

III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

§ 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos."

"Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e

IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

§ 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.

§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014 , os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:

I - tão logo atingida a finalidade de seu uso; ou

II - se encerrado o prazo determinado por obrigação legal.

Art. 14. Para os fins do disposto neste Decreto, considera-se:

I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e

II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Art. 15. Os dados de que trata o art. 11 da Lei nº 12.965, de 2014 , deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto.

Art. 15-A. O dever de guarda de registros de endereço IP pelos provedores de conexão e pelos provedores de aplicações de internet, previsto nos art. 13 e art. 15 da Lei nº 12.965, de 23 de abril de 2014, abrangerá a porta lógica de origem associada sempre que necessário para a identificação inequívoca do terminal de origem ou do próximo enlace de rede. (Incluído pelo Decreto nº 12.975, de 2026)

§ 1º O dever de guarda da porta lógica de origem independerá de prévia requisição e recairá autonomamente sobre cada provedor. (Incluído pelo Decreto nº 12.975, de 2026)

§ 2º O fornecimento da porta lógica de origem e dos dados a ela vinculados observará o disposto nos art. 10 e art. 22 da Lei nº 12.965, de 23 de abril de 2014. (Incluído pelo Decreto nº 12.975, de 2026) "

11. Quanto às competências institucionais, cabe à Anatel regulamentar e fiscalizar os serviços de telecomunicações, nos limites da Lei nº 9.472/1997 e do art. 17 do Decreto nº 8.771/2016. A ANPD atua na proteção de dados pessoais e nas matérias previstas no art. 19-A desse Decreto, enquanto a

Senacon atua na esfera consumerista, conforme o art. 18. Ao Poder Judiciário compete apreciar os pedidos sujeitos à autorização judicial, preservadas as atribuições legais das autoridades de investigação.

Decreto nº 8.771/2016

> "Art. 17. A Anatel atuará na regulação, na fiscalização e na apuração de infrações, nos termos da Lei nº 9.472, de 16 de julho de 1997 .
>
> Art. 18. A Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações, nos termos da Lei nº 8.078, de 11 de setembro de 1990 .
>
> Art. 19. A apuração de infrações à ordem econômica ficará a cargo do Sistema Brasileiro de Defesa da Concorrência, nos termos da Lei nº 12.529, de 30 de novembro de 2011 .
>
> Art. 19-A. A Agência Nacional de Proteção de Dados – ANPD atuará na regulação, na fiscalização e na apuração de infrações quanto à garantia dos direitos dos usuários e ao cumprimento dos deveres dos provedores de aplicações de internet, em especial aqueles previstos nos art. 16-A a 16-P deste Decreto, nos termos: (Incluído pelo Decreto nº 12.975, de 2026)
>
> I - da Lei nº 12.965, de 23 de abril de 2014, especialmente quanto ao disposto nos art. 10 a art. 12; (Incluído pelo Decreto nº 12.975, de 2026)
>
> II - da Lei nº 13.709, de 14 de agosto de 2018; e (Incluído pelo Decreto nº 12.975, de 2026)
>
> III - da Lei nº 15.211, de 17 de setembro de 2025. (Incluído pelo Decreto nº 12.975, de 2026)"

12. À vista dessas disposições, os registros locais descritos na consulta podem atender às obrigações de conservação, mas a confirmação de sua suficiência requer conhecer os serviços de cada agente, seus vínculos com usuários e outras prestadoras, o uso de internet ou numeração pública e os registros e correlações disponíveis, sem exposição de dados pessoais reais. As orientações apresentadas esclarecem os critérios aplicáveis, sem constituir aprovação de implementação específica.

13. Sendo o que tínhamos a informar, colocamo-nos à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

Documento assinado eletronicamente por **Felipe Roberto de Lima**, **Gerente de Regulamentação**, em 13/11/2026, às 18:40, conforme horário oficial de Brasília, com fundamento no art. 4º, inciso I, da Lei nº 14.063/2020 c/c art. 4º, inciso I e § 3º, do Decreto nº 10.543/2020.

A autenticidade deste documento pode ser conferida em https://www.anatel.gov.br/autenticidade, informando o código verificador **16590780** e o código CRC **91139B5C**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 53500.146906/2026-42 SEI nº 16590780