|  |  |  |
| --- | --- | --- |
| **Nama BPR/ BPR Syariah** | : |  |
| **Email Narahubung** | : |  |

| **BATANG TUBUH** | **PENJELASAN** | **TANGGAPAN DAN USULAN PENYESUAIAN** |
| --- | --- | --- |
| PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA  NOMOR … TAHUN 2025  TENTANG  PENYELENGGARAAN TEKNOLOGI INFORMASI  OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH  DENGAN RAHMAT TUHAN YANG MAHA ESA  DEWAN KOMISIONER OTORITAS JASA KEUANGAN, | PENJELASAN  ATAS  PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA  NOMOR … TAHUN 2025  TENTANG  PENYELENGGARAAN TEKNOLOGI INFORMASI  OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH |  |
| Menimbang: | 1. UMUM |  |
| 1. bahwa untuk mendukung proses bisnis dalam melakukan aktivitas operasional guna meningkatkan layanan perbankan kepada masyarakat, dibutuhkan pemanfaatan teknologi informasi oleh bank perekonomian rakyat dan bank perekonomian rakyat syariah; | Dalam era digitalisasi sektor jasa keuangan, pemanfaatan TI merupakan aspek penting dalam kegiatan operasional perbankan. Pemanfaatan TI oleh BPR atau BPR Syariah dilakukan dalam berbagai aktivitas antara lain penghimpunan dana, penyaluran dana maupun kegiatan operasional lain. Perkembangan digitalisasi sektor perbankan juga mendorong industri BPR atau BPR Syariah untuk melakukan transformasi digital melalui pemanfaatan TI secara lebih masif agar operasional BPR atau BPR Syariah lebih andal dan efisien. Selain itu, dorongan untuk melakukan transformasi digital bagi BPR atau BPR Syariah juga semakin mengemuka seiring meningkatnya kebutuhan masyarakat terhadap produk maupun layanan berbasis digital yang dapat diakses tanpa adanya batasan ruang dan waktu.  Pemanfaatan TI oleh BPR atau BPR Syariah memiliki suatu tantangan tersendiri, antara lain risiko terkait kegagalan operasional, ketahanan dan keamanan siber, keterbatasan permodalan serta perlunya peningkatan kualitas sumber daya manusia bidang TI. Peningkatan risiko sebagai dampak pemanfaatan TI yang dihadapi oleh BPR atau BPR Syariah memerlukan suatu peningkatan kapasitas dalam penyelenggaraan TI melalui penerapan tata kelola TI dan manajemen risiko TI secara lebih optimal.  Adopsi TI dalam kegiatan operasional akan meningkatkan peluang kolaborasi antara BPR atau BPR Syariah dengan pihak ketiga termasuk diantaranya pihak penyedia jasa TI maupun penyelenggara inovasi teknologi sektor keuangan. Kolaborasi tersebut perlu dikelola melalui penerapan manajemen risiko yang efektif agar dapat memberikan hasil yang optimal bagi industri BPR atau BPR Syariah. Aspek pelindungan data pribadi maupun pelindungan konsumen juga tetap harus menjadi perhatian utama dalam melakukan kolaborasi dengan pihak ketiga. Selain itu, adanya konektivitas sistem TI milik BPR atau BPR Syariah dengan pihak ketiga akan meningkatkan risiko terkait ketahanan dan keamanan siber yang berpotensi menghambat operasional BPR atau BPR Syariah.  Tingginya disparitas BPR atau BPR Syariah dari segi permodalan maupun kualitas sumber daya manusia bidang TI menyebabkan kondisi penyelenggaraan TI BPR atau BPR Syariah memiliki kesenjangan yang cukup beragam, sehingga diperlukan suatu standar regulasi yang komprehensif untuk menjawab tantangan dalam penyelenggaraan TI. Sehubungan dengan hal tersebut, perlu dilakukan penyusunan pengaturan tentang penyelenggaraan teknologi informasi oleh BPR dan BPR Syariah. |  |
| 1. bahwa pemanfaatan teknologi informasi berpotensi meningkatkan risiko terkait kegagalan operasional bagi bank perekonomian rakyat dan bank perekonomian rakyat syariah sehingga diperlukan penguatan aspek tata kelola dan manajemen risiko dalam penyelenggaraan teknologi informasi; |
| 1. bahwa dibutuhkan pengaturan aspek tata kelola, manajemen risiko, ketahanan dan keamanan siber dalam penyelenggaraan teknologi informasi, sehingga perlu mengganti Peraturan Otoritas Jasa Keuangan Nomor 75 /POJK.03/2016 tentang Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah; |
| 1. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah; |
| Mengingat: |
| 1. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 3472) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6845); |
| 1. Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 94, Tambahan Lembaran Negara Republik Indonesia Nomor 4867) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6845); |
| 1. Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 5253) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6845); |
| Memutuskan: |
| Menetapkan : PERATURAN OTORITAS JASA KEUANGAN TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI OLEH BANK PEREKONOMIAN RAKYAT DAN BANK PEREKONOMIAN RAKYAT SYARIAH |
|  |  |  |
| **BAB I** |  |  |
| **KETENTUAN UMUM** |  |  |
| **Pasal 1** | **Pasal 1** |  |
| Dalam Peraturan Otoritas Jasa Keuangan ini, yang dimaksud dengan: | Cukup jelas. |  |
| 1. Bank Perekonomian Rakyat yang selanjutnya disingkat BPR adalah bank konvensional yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas giral secara langsung. |  |  |
| 1. Bank Perekonomian Rakyat Syariah yang selanjutnya disebut BPR Syariah adalah jenis bank syariah yang dalam kegiatannya tidak memberikan jasa dalam lalu lintas giral secara langsung |  |  |
| 1. Teknologi Informasi yang selanjutnya disingkat TI adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi. |  |  |
| 1. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. |  |  |
| 1. Pusat Data (*Data Center*) adalah suatu fasilitas yang digunakan untuk menempatkan Sistem Elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data. |  |  |
| 1. Pusat Pemulihan Bencana (*Disaster Recovery Center*) adalah suatu fasilitas yang digunakan untuk memulihkan kembali data atau informasi serta fungsi-fungsi penting Sistem Elektronik yang terganggu atau rusak akibat terjadinya bencana yang disebabkan oleh alam atau manusia. |  |  |
| 1. Rencana Pemulihan Bencana adalah dokumen yang berisikan rencana dan langkah untuk menggantikan dan/atau memulihkan kembali akses data, perangkat keras, dan perangkat lunak yang diperlukan, agar BPR atau BPR Syariah dapat menjalankan kegiatan operasional bisnis yang kritikal setelah adanya gangguan dan/atau bencana. |  |  |
| 1. Direksi adalah direksi bagi BPR atau BPR Syariah berbentuk badan hukum perseroan terbatas, perusahaan umum daerah, perusahaan perseroan daerah, perusahaan daerah, atau pengurus bagi BPR atau BPR Syariah berbentuk badan hukum koperasi. |  |  |
| 1. Dewan Komisaris adalah dewan komisaris bagi BPR atau BPR Syariah berbentuk badan hukum perseroan terbatas, komisaris bagi BPR atau BPR Syariah berbentuk badan hukum perusahaan perseroan daerah, dewan pengawas bagi BPR berbentuk badan hukum perusahaan umum daerah dan perusahaan daerah, serta pengawas bagi BPR atau BPR Syariah berbentuk badan hukum koperasi. |  |  |
|  |  |  |
| **BAB II** |  |  |
| **TATA KELOLA TI BPR DAN BPR SYARIAH** |  |  |
| **Bagian Kesatu** |  |  |
| **Penerapan Tata Kelola TI BPR dan BPR Syariah** |  |  |
| **Pasal 2** | **Pasal 2** |  |
| 1. BPR atau BPR Syariah wajib menerapkan tata kelola TI yang baik dalam penyelenggaraan TI. | Ayat (1)  Penerapan tata kelola TI merupakan bagian dari penerapan tata kelola BPR atau BPR Syariah secara umum. Tata kelola yang baik dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola bagi BPR dan BPR Syariah.  Tata kelola TI diterapkan pada seluruh kegiatan yang berkaitan dengan penyelenggaraan TI antara lain manajemen risiko, pengelolaan data, penggunaan pihak penyedia jasa TI, pengendalian intern, serta pengembangan dan perubahan TI.  Dalam menerapkan tata kelola TI, BPR atau BPR Syariah melakukan pemetaan atas aspek antara lain:   1. proses bisnis; 2. struktur organisasi; 3. kebijakan, standar, dan prosedur; 4. sumber daya manusia pendukung; dan 5. infrastruktur dan aplikasi. |  |
| 1. Dalam menerapkan tata kelola TI yang baik sebagaimana dimaksud pada ayat (1), BPR atau BPR Syariah mempertimbangkan faktor paling sedikit: 2. strategi dan tujuan bisnis BPR atau BPR Syariah; 3. skala usaha dan kompleksitas bisnis BPR atau BPR Syariah; 4. peran TI bagi BPR atau BPR Syariah; 5. metode pengadaan sumber daya TI; 6. risiko dan permasalahan terkait TI; 7. praktik atau standar yang berlaku secara nasional maupun internasional; dan 8. ketentuan peraturan perundang-undangan. | Ayat (2)  Huruf a  Strategi dan tujuan bisnis BPR atau BPR Syariah mencerminkan antara lain arah bisnis dan kebutuhan dari pemangku kepentingan.  Huruf b  Cukup jelas.  Huruf c  Cukup jelas.  Huruf d  Metode pengadaan sumber daya TI disesuaikan dengan kebutuhan dan kemampuan BPR atau BPR Syariah, antara lain pengadaan secara mandiri, pengadaan dengan menggunakan pihak penyedia jasa TI, dan kombinasi antara keduanya.  Huruf e  Cukup jelas.  Huruf f  Cukup jelas.  Huruf g  Cukup jelas. |  |
| 1. Dalam menerapkan tata kelola TI yang baik sebagaimana dimaksud pada ayat (1), BPR atau BPRS Syariah melakukan kegiatan paling sedikit: 2. perencanaan dan pelaksanaan aktivitas yang mendukung kegiatan penyelenggaraan TI; 3. implementasi layanan TI secara optimal agar dapat terintegrasi dalam proses bisnis BPR atau BPR Syariah; dan 4. penyediaan dukungan operasional layanan TI kepada seluruh pengguna layanan TI. | Ayat (3)  Cukup jelas. |  |
| **Pasal 3** | **Pasal 3** |  |
| BPR atau BPR Syariah wajib menetapkan wewenang dan tanggung jawab yang jelas dari Direksi, Dewan Komisaris, dan pejabat terkait dengan penerapan tata kelola TI. | Cukup jelas. |  |
| **Pasal 4** | **Pasal 4** |  |
| Wewenang dan tanggung jawab Direksi sebagaimana dimaksud dalam Pasal 3 paling sedikit:   1. menetapkan rencana pengembangan dan pengadaan TI BPR atau BPR Syariah; 2. menetapkan kebijakan dan prosedur terkait penyelenggaraan TI yang memadai dan mengkomunikasikannya secara efektif, baik pada satuan kerja penyelenggara maupun pengguna TI; 3. memantau kecukupan kinerja penyelenggaraan TI dan upaya peningkatannya; dan 4. memastikan bahwa: 5. TI yang digunakan mendukung perkembangan usaha, pencapaian tujuan bisnis dan kelangsungan pelayanan terhadap nasabah BPR atau BPR Syariah; 6. terdapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan TI; 7. tersedianya sistem pengelolaan pengamanan informasi (*information security management system*) yang efektif dan dikomunikasikan kepada satuan kerja penyelenggara dan pengguna TI; dan 8. kebijakan dan prosedur penyelenggaraan TI diterapkan secara efektif. | Cukup jelas. |  |
| **Pasal 5** | **Pasal 5** |  |
| Wewenang dan tanggung jawab Dewan Komisaris sebagaimana dimaksud dalam Pasal 3 paling sedikit:   1. mengarahkan dan memantau rencana pengembangan dan pengadaan TI BPR atau BPR Syariah yang bersifat mendasar; 2. mengevaluasi pertanggungjawaban Direksi terkait penyelenggaraan TI BPR atau BPR Syariah; dan 3. mengarahkan dan memantau penerapan tata kelola TI BPR atau BPR Syairah. | Huruf a  Yang dimaksud dengan “pengembangan TI” adalah proses pengembangan sistem TI baru termasuk penggantian atau perbaikan sistem teknologi yang telah ada, baik dilakukan secara mandiri oleh BPR atau BPRS maupun bekerja sama dengan penyedia jasa TI.  Yang dimaksud dengan “pengadaan TI” adalah proses pemenuhan atau penyediaan barang dan/atau jasa terkait TI. Termasuk dalam pengembangan dan pengadaan TI yang bersifat mendasar antara lain perubahan secara signifikan terhadap konfigurasi TI atau aplikasi inti perbankan (c*ore banking system*), pengadaan aplikasi inti perbankan baru, kerja sama dengan penyedia jasa TI, serta pengembangan dan pengadaan TI mendasar lainnya yang dapat menambah dan/atau meningkatkan risiko BPR atau BPR Syariah.  Huruf b  Cukup jelas.  Huruf c  Cukup jelas. |  |
| **Pasal 6** | **Pasal 6** |  |
| 1. BPR dan BPR Syariah wajib memiliki kebijakan dan prosedur penyelenggaraan TI. | Ayat (1)  Cukup jelas. |  |
| 1. Kebijakan dan prosedur penyelenggaraan TI sebagaimana dimaksud pada ayat (1) paling sedikit meliputi: 2. wewenang dan tanggung jawab Direksi, Dewan Komisaris, dan Satuan Kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI; 3. pengembangan dan pengadaan; 4. operasional TI; 5. jaringan komunikasi; 6. pengamanan informasi; 7. Rencana Pemulihan Bencana; 8. audit intern TI; dan 9. penggunaan pihak penyedia jasa TI. | Ayat (2)  Huruf a  Cukup jelas.  Huruf b  Cukup jelas.  Huruf c  Cukup jelas.  Huruf d  Cukup jelas.  Huruf e  Cukup jelas.  Huruf f  Cukup jelas.  Huruf g  Cukup jelas.  Huruf h  Kebijakan dan prosedur dalam penggunaan pihak penyedia jasa TI memuat antara lain:   1. proses identifikasi kebutuhan penggunaan pihak penyedia jasa TI; 2. proses pemilihan pihak penyedia jasa TI; dan 3. tata cara melakukan hubungan kerja sama dengan pihak penyedia jasa TI. |  |
| **Bagian Kedua** |  |  |
| **Satuan Kerja Penyelenggara TI** |  |  |
| **Pasal 7** | **Pasal 7** |  |
| 1. BPR atau BPR Syariah wajib menunjuk satuan kerja atau fungsi yang bertanggung jawab atas penyelenggaraan TI. | Ayat (1)  Fungsi antara lain pegawai yang bertanggung jawab atas penyelenggaraan TI BPR atau BPR Syariah. |  |
| 1. Satuan kerja atau fungsi yang bertanggung jawab atas penyelenggaraan TI sebagaimana dimaksud pada ayat (1) ditempatkan pada fungsi operasional sesuai Peraturan Otoritas Jasa Keuangan mengenai tata kelola bagi BPR dan BPR Syariah. | Ayat (2)  Cukup jelas. |  |
| 1. Penyelenggaraan TI sebagaimana dimaksud pada ayat (1) paling sedikit berupa aktivitas: 2. perencanaan kebutuhan infrastruktur TI; 3. penyusunan atau pengembangan Sistem Elektronik, termasuk aplikasi yang menunjang bisnis BPR atau BPR Syariah; 4. pengoperasian TI; dan 5. pemantauan atas kegiatan penyelenggaraan TI. | Ayat (3)  Cukup jelas. |  |
| 1. Bagi BPR atau BPR Syariah yang menyediakan layanan digital wajib memiliki satuan kerja penyelenggaraan TI yang dipimpin oleh pejabat eksekutif. | Ayat (4)  Cukup jelas. |  |
| 1. Satuan kerja penyelenggaraan TI BPR atau BPR Syariah sebagaimana dimaksud ayat (1) dan (4) disesuaikan dengan skala usaha dan kompleksitas TI BPR atau BPR Syariah. | Ayat (5)  Cukup jelas. |  |
| **Pasal 8** | **Pasal 8** |  |
| Wewenang dan tanggung jawab satuan kerja atau fungsi yang bertanggung jawab terhadap penyelenggaraan TI BPR atau BPR Syariah sebagaimana dimaksud dalam Pasal 7 ayat (1) paling sedikit:   1. membantu Direksi dan Dewan Komisaris dalam penyelenggaraan TI terkait dengan perencanaan, pelaksanaan dan pemantauan; 2. mendukung pengembangan dan/atau pengadaan TI; 3. mendukung implementasi, operasional, dan pemeliharaan TI; dan 4. melakukan upaya penyelesaian permasalahan terkait operasional TI, yang tidak dapat diselesaikan oleh satuan kerja pengguna TI. | Cukup jelas. |  |
| **Pasal 9** | **Pasal 9** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 2 ayat (1), Pasal 3, Pasal 6 ayat (1), Pasal 7 ayat (1) dan/atau ayat (4) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 2 ayat (1), Pasal 3, Pasal 6 ayat (1), Pasal 7 ayat (1) dan/atau ayat (4), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 10** | **Pasal 10** |  |
| Ketentuan lebih lanjut mengenai penerapan tata kelola TI ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB III** |  |  |
| **ARSITEKTUR TI BPR DAN BPR SYARIAH** |  |  |
| **Pasal 11** | **Pasal 11** |  |
| 1. BPR atau BPR Syariah yang menyediakan layanan digital wajib memiliki arsitektur TI. | Ayat (1)  Yang dimaksud dengan “layanan digital” adalah produk dalam bentuk layanan yang diberikan oleh BPR atau BPR Syariah dengan pemanfaatan TI melalui media elektronik untuk memberikan akses bagi nasabah dan/atau calon nasabah terkait produk BPR atau BPR Syariah maupun produk dan/atau layanan dari mitra BPR atau BPR Syariah, serta dapat dilakukan secara mandiri oleh nasabah dan/atau calon nasabah.  Contoh layanan digital antara lain *mobile banking* dan *internet banking*.  Yang dimaksud dengan “arsitektur TI” adalah bagan yang menggambarkan hubungan antar seluruh infrastruktur TI yang dimiliki dan/ atau dikelola oleh BPR atau BPR Syariah. Infrastruktur TI antara lain Pusat Data, aplikasi inti perbankan dan aplikasi terkait layanan digital. |  |
| 1. Arsitektur TI sebagaimana dimaksud pada ayat (1) disetujui oleh Direksi BPR atau BPR Syariah. | Ayat (2)  Cukup jelas. |  |
| 1. BPR atau BPR syariah wajib memiliki prosedur internal mengenai mekanisme penginian arsitektur TI. | Ayat (3)  Prosedur perubahan arsitektur TI dapat menjadi bagian dari prosedur penyelenggaraan TI BPR atau BPR Syariah. Perubahan arsitektur TI disetujui oleh Direksi BPR atau BPR Syariah |  |
| **Pasal 12** | **Pasal 12** |  |
| 1. Dalam menyusun arsitektur TI sebagaimana dimaksud dalam Pasal 10 ayat (1), BPR atau BPR Syariah mempertimbangkan rencana bisnis BPR atau BPR Syariah. | Ayat (1)  Cukup jelas. |  |
| 1. Arsitektur TI dapat disusun oleh BPR atau BPR Syariah secara mandiri maupun bekerja sama dengan pihak ketiga. | Ayat (2)  Yang dimaksud "pihak ketiga" antara lain pihak penyedia jasa TI maupun individu/perorangan yang memiliki keahlian dalam menyusun arsitektur TI. |  |
| 1. Ketentuan lebih lanjut mengenai penyusunan arsitektur TI ditetapkan oleh Otoritas Jasa Keuangan. | Ayat (3)  Cukup jelas. |  |
| **Pasal 13** | **Pasal 13** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1), dan/atau ayat (3) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1), dan/atau ayat (3), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
|  |  |  |
| **BAB IV** |  |  |
| **PENERAPAN MANAJEMEN RISIKO PENYELENGGARAAN TI BPR DAN BPR SYARIAH** |  |  |
| **Bagian Kesatu** |  |  |
| **Umum** |  |  |
| **Pasal 14** | **Pasal 14** |  |
| 1. BPR atau BPR Syariah wajib menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI. | Ayat (1)  Cakupan penerapan manajemen risiko secara efektif dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi BPR atau Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi BPR Syariah.  Manajemen risiko berlaku untuk seluruh penyelenggaraan TI antara lain:   1. keamanan siber; 2. pengelolaan data; 3. penggunaan pihak penyedia jasa TI; dan 4. operasional TI. |  |
| 1. BPR atau BPR Syariah wajib memastikan kecukupan sistem informasi manajemen risiko dalam penyelenggaraan TI. | Ayat (2)  Cukup jelas. |  |
| **Bagian Kedua** |  |  |
| **Pengamanan Informasi dalam Penyelenggaraan TI BPR dan BPR Syariah** |  |  |
| **Pasal 15** | **Pasal 15** |  |
| 1. BPR atau BPR Syariah wajib memastikan pengamanan informasi dilaksanakan secara efektif dan efisien. | Ayat (1)  Pengamanan informasi ditujukan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikelola.  Pengamanan informasi diperlukan untuk mencegah gangguan keamanan dalam penyelenggaraan TI yang berpotensi merugikan BPR, BPRS dan/atau nasabahnya. |  |
| 1. Pengamanan informasi sebagaimana dimaksud pada ayat (1) dilakukan terhadap aspek sumber daya manusia, proses, teknologi, dan fisik atau lingkungan, dalam penyelenggaraan TI secara menyeluruh. | Ayat (2)  Contoh pengamanan informasi terhadap aspek sumber daya manusia antara lain adanya prosedur pemberian hak akses terhadap informasi sesuai dengan kewenangan pegawai BPR atau BPR Syariah.  Contoh pengamanan informasi terhadap aspek proses antara lain pengelolaan pengguna (*user*) untuk memantau akses pengguna terhadap perangkat lunak atau aplikasi milik BPR atau BPR Syariah.  Contoh pengamanan informasi terhadap aspek teknologi antara lain penggunaan *anti virus* pada *end point* (PC/ komputer).  Contoh pengamanan informasi terhadap aspek fisik atau lingkungan antara lain pembatasan hak akses kepada pihak yang tidak berwenang terhadap infrastruktur TI milik BPR atau BPR Syariah. |  |
| 1. BPR dan BPR Syariah wajib melakukan pengendalian otorisasi (*authorization of control*) dalam penyelenggaraan TI. | Ayat (3)  Yang dimaksud dengan “pengendalian otorisasi” adalah memastikan adanya pengendalian terhadap hak akses dan otorisasi yang tepat terhadap sistem, pangkalan data (*database*), dan aplikasi yang digunakan. Seluruh arsip dan data yang bersifat rahasia hanya dapat diakses oleh pihak yang telah memiliki otoritas serta harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi oleh pihak yang tidak berwenang. |  |
| **Pasal 16** | **Pasal 16** |  |
| BPR atau BPR Syariah wajib memastikan jaringan komunikasi yang disediakan oleh BPR atau BPR Syariah telah memenuhi prinsip kerahasiaan, integritas, dan ketersediaan. | Yang dimaksud dengan prinsip “kerahasiaan” adalah memastikan bahwa metode dan prosedur yang dimiliki dapat melindungi kerahasiaan data nasabah.  Yang dimaksud dengan prinsip “integritas” adalah memastikan bahwa metode dan prosedur yang dimiliki mampu melindungi data sehingga menjadi akurat, handal, konsisten, dan terbukti kebenarannya agar terhindar dari kesalahan, kecurangan, manipulasi, penyalahgunaan, dan perusakan data.  Yang dimaksud dengan prinsip “ketersediaan” adalah memastikan ketersediaan sistem secara berkesinambungan. |  |
| **Pasal 17** | **Pasal 17** |  |
| 1. BPR atau BPR Syariah wajib memiliki Rencana Pemulihan Bencana yang teruji dan memadai. | Ayat (1)  Cukup jelas. |  |
| 1. Rencana Pemulihan Bencana sebagaimana dimaksud pada ayat (1) harus dapat dilaksanakan secara efektif agar operasional BPR atau BPR Syariah tetap berjalan saat terjadi gangguan dan/atau bencana yang signifikan pada sarana TI yang digunakan. | Ayat (2)  Rencana Pemulihan Bencana mencakup rencana pemulihan pada berbagai tingkat bencana dan gangguan seperti:   1. *minor disaster* yang berdampak kecil dan tidak memerlukan biaya besar serta dapat diselesaikan dalam jangka waktu pendek; 2. *major disaster* yang berdampak besar dan dapat menjadi lebih parah apabila tidak diatasi segera; dan/atau 3. *catastrophic disaster* yang berdampak terjadi kerusakan yang bersifat permanen sehingga memerlukan relokasi atau penggantian dengan biaya yang besar.   Yang dimaksud dengan “dapat dilaksanakan secara efektif” adalah operasional TI dapat berjalan kembali segera setelah gangguan dan/atau bencana terjadi sehingga tidak mengganggu pelayanan kepada nasabah. |  |
| 1. BPR atau BPR Syariah sebagaimana dimaksud pada ayat (1) wajib melakukan uji coba atas Rencana Pemulihan Bencana terhadap seluruh aplikasi dan infrastruktur yang kritikal sesuai hasil analisis dampak bisnis, paling sedikit 1 (satu) kali dalam 3 (tiga) tahun dengan melibatkan pengguna TI. | Ayat (3)  Cukup jelas. |  |
| 1. BPR atau BPR Syariah wajib melakukan kaji ulang Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 3 (tiga) tahun dengan mempertimbangkan hasil uji coba sebagaimana dimaksud pada ayat (3). | Ayat (4)  Kaji ulang terhadap Rencana Pemulihan Bencana dilakukan terhadap seluruh atau sebagian aspek yang terkait antara lain dalam hal terdapat perubahan aplikasi yang signifikan, dan perubahan lokasi Pusat Data/ Pusat Pemulihan Bencana. |  |
| **Pasal 18** | **Pasal 18** |  |
| 1. BPR atau BPR Syariah yang: 2. memiliki modal inti paling sedikit Rp50.000.000.000,00 (lima puluh miliar rupiah); dan/atau 3. menyediakan layanan digital,   wajib menyediakan Pusat Pemulihan Bencana. | Cukup jelas. |  |
| 1. Pusat Pemulihan Bencana sebagaimana dimaksud pada ayat (1) dapat dimiliki oleh BPR atau BPR Syariah secara mandiri maupun bekerjasama dengan pihak penyedia jasa TI. |  |  |
| **Pasal 19** | **Pasal 19** |  |
| 1. BPR atau BPR Syariah yang menyelenggarakan TI secara mandiri wajib: 2. melakukan rekam cadang (*back* u*p*) data aktivitas yang diproses menggunakan TI; dan 3. memiliki *installer* aplikasi inti perbankan yang digunakan BPR atau BPR Syariah untuk melakukan *install* ulang. | Ayat (1)  Huruf a  Yang dimaksud dengan “rekam cadang” adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data komputer dalam media penyimpan elektronik, termasuk namun tidak terbatas pada media penyimpan seperti *hardisk*, *flashdisk*, dan/atau *compact dis*k, sehingga data tersebut dapat ditampilkan kembali. Media penyimpan tidak termasuk media penyimpan online publik. Rekam cadang bertujuan untuk mengembalikan data apabila data tersebut hilang, baik karena terhapus atau rusak (*corrupt*), serta untuk mengembalikan data ke posisi tertentu.  Huruf b  Yang dimaksud *installer a*plikasi inti perbankan yaitu perangkat lunak yang dapat dilakukan *install* kembali apabila diperlukan. |  |
| 1. BPR dan BPRS yang menggunakan pihak penyedia jasa TI dalam penyelenggaraan TI, wajib memastikan bahwa pihak penyedia jasa TI melakukan rekam cadang (*back up*) data aktivitas dan memiliki *installer* aplikasi inti perbankan. | Ayat (2)  Cukup jelas. |  |
| 1. BPR dan BPR Syariah wajib menyimpan data aktivitas sebagaimana dimaksud pada ayat (1) dan ayat (2) dalam jangka waktu sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. | Ayat (3)  Ketentuan peraturan perundang-undangan antara lain peraturan perundang-undangan mengenai dokumen perusahaan. |  |
| 1. BPR dan BPR Syariah wajib melakukan rekam cadang sebagaimana dimaksud pada ayat (1) huruf a dan ayat (2) setiap akhir hari untuk seluruh data aktivitas BPR dan BPR Syariah. | Ayat (4)  Cukup jelas. |  |
| **Pasal 20** | **Pasal 20** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 14, Pasal 15 ayat (1), ayat (3), Pasal 16, Pasal 17 ayat (1), ayat (3), ayat (4), Pasal 18 ayat (1), dan/atau Pasal 19 dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 14, Pasal 15 ayat (1), ayat (3), Pasal 16, Pasal 17 ayat (1), ayat (3), ayat (4), Pasal 18 ayat (1), dan/atau Pasal 19, BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 21** | **Pasal 21** |  |
| Ketentuan lebih lanjut mengenai penerapan manajemen risiko dalam penyelenggaraan TI ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB V** |  |  |
| **KETAHANAN DAN KEMANAN SIBER** |  |  |
| **Pasal 22** | **Pasal 22** |  |
| 1. BPR atau BPR Syariah wajib menjaga ketahanan siber. | Ayat (1)  Cukup jelas. |  |
| 1. Untuk menjaga ketahanan siber sebagaimana dimaksud pada ayat (1), BPR atau BPR Syariah melakukan proses paling sedikit: 2. identifikasi aset, ancaman, dan kerentanan; 3. pelindungan aset; 4. deteksi insiden siber; dan 5. penanggulangan dan pemulihan insiden siber. | Ayat (2)  Huruf a  Proses identifikasi aset, ancaman, dan kerentanan antara lain melakukan pemantauan terhadap perkembangan siber yang terkini, baik dari sisi teknologi, taktik dan teknik serangan, serta prosedur atau pola serangan, untuk mengidentifikasi ancaman siber.  Huruf b  Proses pelindungan aset antara lain menerapkan pengendalian keamanan *(security control*) yang komprehensif sesuai hasil identifikasi aset, ancaman, dan kerentanan.  Huruf c  Proses deteksi insiden siber antara lain melakukan pemantauan atas aktivitas mencurigakan serta melakukan pengujian terhadap proses dan prosedur deteksi untuk memastikan aktivitas anomali dapat dideteksi tepat waktu.  Huruf d  Proses penanggulangan dan pemulihan insiden siber antara lain menerapkan prosedur pemulihan serta upaya untuk mencegah penyebaran dampak dari suatu insiden siber. |  |
| 1. BPR atau BPR Syariah memastikan proses untuk menjaga ketahanan siber sebagaimana dimaksud pada ayat (2) didukung dengan sistem informasi ketahanan siber yang memadai. | Ayat (3)  Yang dimaksud dengan “sistem informasi ketahanan siber yang memadai” adalah sistem informasi yang dapat mendukung keseluruhan proses dalam menjaga ketahanan siber, sesuai dengan ukuran dan kompleksitas bisnis BPR atau BPR Syariah |  |
| 1. Ketentuan lebih lanjut mengenai ketahanan dan keamanan siber ditetapkan oleh Otoritas Jasa Keuangan. | Ayat (4)  Cukup jelas. |  |
| **Pasal 23** | **Pasal 23** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22 ayat (1) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 22 ayat (1), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
|  |  |  |
| **BAB VI** |  |  |
| **PENGGUNAAN PIHAK PENYEDIA JASA TI DALAM PENYELENGGARAAN TI BPR DAN BPR SYARIAH** |  |  |
| **Pasal 24** | **Pasal 24** |  |
| 1. BPR atau BPR Syariah dapat menggunakan pihak penyedia jasa TI dalam penyelenggaraan TI. | Ayat (1)  Yang dimaksud dengan “menggunakan pihak penyedia jasa TI” adalah penggunaan jasa pihak lain dalam penyelenggaraan TI BPR atau BPR Syariah secara berkesinambungan dan/atau dalam periode tertentu. Selain itu, meskipun BPR atau BPR Syariah menyerahkan penyelenggaraan TI kepada pihak penyedia jasa TI maka BPR atau BPR Syariah tetap bertindak sebagai penyelenggara Sistem Elektronik untuk setiap Sistem Elektronik yang digunakan BPR atau BPR Syariah dalam menjalankan kegiatan usahanya. Contoh penyelenggaraan TI yang menggunakan pihak penyedia jasa TI antara lain penggunaan komputasi awan (*cloud computing*). |  |
| 1. Dalam penggunaan pihak penyedia jasa TI sebagaimana dimaksud pada ayat (1), BPR atau BPR Syariah wajib: 2. bertanggung jawab terhadap penyelenggaraan TI; 3. memiliki kemampuan dan melakukan pengawasan terhadap penyelenggaraan TI BPR atau BPR Syariah yang diselenggarakan oleh pihak penyedia jasa TI; 4. memantau reputasi pihak penyedia jasa TI dan kelangsungan penyediaan layanan kepada BPR atau BPR Syariah; 5. memilih pihak penyedia jasa TI berdasarkan analisis manfaat dan biaya dengan melibatkan satuan kerja atau pegawai yang bertanggung jawab terhadap penyelenggaraan TI; 6. memberikan akses kepada Otoritas Jasa Keuangan terhadap pangkalan data secara tepat waktu baik untuk data terkini maupun untuk data yang telah lalu; 7. memastikan penyedia jasa TI: 8. memiliki tenaga ahli yang didukung dengan sertifikat keahlian sesuai dengan keperluan penyelenggaraan TI; 9. menerapkan prinsip pengendalian TI secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen; 10. menyediakan akses bagi auditor intern BPR dan BPRS, auditor ekstern yang ditunjuk oleh BPR dan BPRS, dan Otoritas Jasa Keuangan untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan; 11. menyatakan tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang sesuai dengan ketentuan peraturan perundang-undangan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan; 12. menjaga keamanan seluruh data dan informasi termasuk data pribadi nasabah; 13. melaporkan kepada BPR atau BPRS setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan dan/atau mengganggu kelangsungan operasional BPR atau BPRS; 14. menyediakan Rencana Pemulihan Bencana yang teruji dan memadai; 15. mekanisme penghentian kerja sama (*exit clause*) dengan pihak penyedia jasa TI ; 16. bersedia untuk menyepakati kemungkinan penghentian perjanjian kerja sama sebelum berakhirnya jangka waktu perjanjian (*early termination*) dalam hal perjanjian kerja sama tersebut menyebabkan atau diindikasikan akan menyebabkan kesulitan pelaksanaan tugas pengawasan Otoritas Jasa Keuangan; dan 17. memenuhi tingkat layanan sesuai dengan perjanjian tingkat layanan (*service level agreement*) antara BPR atau BPRS dan pihak penyedia jasa TI. | Ayat (2)  Huruf a  Cukup jelas.  Huruf b  Kemampuan dalam melakukan pengawasan terhadap penyelenggaraan TI BPR atau BPRS yang diselenggarakan oleh pihak penyedia jasa TI antara lain ditunjukkan dengan tersedianya sumber daya manusia yang memiliki pengetahuan atau kapabilitas mengenai jasa TI yang diberikan oleh pihak penyedia jasa TI.  Huruf c  Pemantauan terhadap reputasi pihak penyedia jasa TI dapat dilakukan berdasarkan informasi yang diperoleh dari berbagai sumber baik intern maupun ekstern.  Huruf d  Cukup jelas.  Huruf e  Akses terhadap pangkalan data meliputi namun tidak terbatas pada penyediaan terminal, *user* *id*, dan sandi lewat (*password*) untuk melakukan *query* dan unduh data (*download* data).  Huruf f  Angka 1  Cukup jelas.  Angka 2  Pengendalian TI dimaksudkan untuk meyakini bahwa aplikasi inti perbankan, Pusat Data dan Pusat Pemulihan Bencana yang digunakan oleh BPR dan BPRS memiliki pengendalian TI yang memadai paling sedikit meliputi *physical security* dan *logical security*.  Angka 3  Cukup jelas.  Angka 4  Cukup jelas.  Angka 5  Contoh keamanan data dan/atau informasi yaitu:   1. pengelolaan akses; 2. manajemen enkripsi dan sandi; 3. keamanan jaringan komunikasi; dan 4. kerahasiaan data pribadi nasabah BPR atau BPR Syariah.   Angka 6  Yang dimaksud “kejadian kritis” adalah kegagalan sistem yang serius, *system down time* dan degradasi kinerja sistem yang memengaruhi kinerja BPR atau BPRS dalam memberikan pelayanan kepada nasabah.  Angka 7  Cukup jelas.  Angka 8  Penghentian perjanjian kerja sama (*exit clause*) termasuk jika terdapat penghentian perjanjian sebelum jangka waktu perjanjian berakhir.  Mekanisme penghentian kerja sama dengan pihak penyedia jasa TI termasuk *escrow agreement.*  *Escrow agreement* yaitu perjanjian yang memungkinkan pemberian hak kepada pembeli perangkat lunak untuk dapat memiliki kode sumber (*source code)* versi terkini dalam hal perusahaan pembuat sistem aplikasi tidak beroperasi lagi.  Angka 9  Cukup jelas.  Angka 10  Pemenuhan tingkat layanan dilakukan guna memastikan penyelenggaraan TI dapat mendukung BPR dan BPR Syariah beroperasi sebagaimana mestinya. |  |
| 1. BPR atau BPR syariah dalam melakukan hubungan kerja sama dengan pihak penyedia jasa TI sebagaimana dimaksud pada ayat (1) wajib didasarkan pada perjanjian kerja sama yang paling sedikit memuat: 2. cakupan pekerjaan atau jasa dalam penyelenggaraan TI; 3. hak dan kewajiban BPR atau BPR Syariah maupun pihak penyedia jasa TI; dan 4. pokok-pokok perjanjian kerja sama, termasuk ketentuan sebagaimana dimaksud pada ayat (2) huruf f. | Ayat (3)  Cukup jelas. |  |
| 1. BPR dan BPR Syariah wajib memastikan bahwa penyedia jasa TI sebagaimana dimaksud pada ayat (1) berbentuk badan hukum yang berkedudukan di wilayah Indonesia. | Ayat (4)  Cukup jelas. |  |
| 1. BPR dan BPR Syariah wajib memastikan penyedia jasa TI sebagaimana dimaksud pada ayat (1) tidak melakukan pengalihan (subkontrak) sebagian atau seluruh kegiatan penyelenggaraan TI BPR atau BPR Syariah kepada pihak lain. | Ayat (5)  Cukup jelas. |  |
| **Pasal 25** | **Pasal 25** |  |
| 1. Dalam hal terdapat kondisi berupa: 2. memburuknya kinerja penyelenggaraan TI oleh pihak penyedia jasa TI yang berpotensi menimbulkan dan/atau mengakibatkan dampak yang signifikan pada kegiatan usaha dan/atau operasional BPR atau BPR Syariah; 3. pihak penyedia jasa TI menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan; 4. terdapat pelanggaran oleh pihak penyedia jasa TI terhadap ketentuan peraturan perundang-undangan; 5. terdapat kondisi yang menyebabkan BPR atau BPR Syariah tidak dapat menyediakan data dan informasi yang diperlukan untuk pengawasan oleh Otoritas Jasa Keuangan; dan/atau 6. terdapat kondisi lain yang menyebabkan terganggunya atau terhentinya penyediaan jasa TI dari pihak penyedia jasa TI kepada BPR atau BPR Syariah,   BPR atau BPR Syariah wajib melakukan tindakan tertentu. | Ayat (1)  Huruf a  Cukup jelas.  Huruf b  Yang dimaksud dengan “insolven” adalah tidak memiliki cukup dana untuk melunasi utang.  Huruf c  Ketentuan peraturan perundang-undangan antara lain mengenai rahasia bank dan/atau pelindungan data pribadi.  Huruf d  Cukup jelas.  Huruf e  Cukup jelas. |  |
| 1. Tindakan tertentu sebagaimana dimaksud pada ayat (1), paling sedikit: 2. melaporkan kepada Otoritas Jasa Keuangan paling lama 3 (tiga) hari kerja setelah kondisi sebagaimana dimaksud pada ayat (1) diketahui oleh BPR atau BPR Syariah; 3. memutuskan tindak lanjut yang akan diambil untuk mengatasi permasalahan termasuk penghentian penggunaan pihak penyedia jasa TI dalam hal diperlukan; dan 4. melaporkan kepada Otoritas Jasa Keuangan paling lama 10 (sepuluh) hari kerja setelah BPR atau BPR Syariah menghentikan penggunaan pihak penyedia jasa TI sebelum berakhirnya jangka waktu perjanjian, dalam hal BPR atau BPR Syariah memutuskan untuk menghentikan penggunaan pihak penyedia jasa TI. | Ayat (2)  Cukup jelas. |  |
| 1. Dalam hal penggunaan pihak penyedia jasa TI menyebabkan atau diindikasikan akan menyebabkan kesulitan pengawasan yang dilakukan oleh Otoritas Jasa Keuangan, Otoritas Jasa Keuangan dapat: 2. meminta BPR atau BPR Syariah untuk melakukan upaya perbaikan melalui penyampaian rencana tindak; dan/atau 3. memerintahkan BPR atau BPR Syariah untuk menghentikan penggunaan pihak penyedia jasa TI sebelum berakhirnya jangka waktu perjanjian. | Ayat (3)  Indikasi kesulitan pengawasan antara lain:   1. kesulitan dalam memperoleh akses terhadap data dan/atau informasi; 2. kesulitan dalam pelaksanaan pemeriksaan terhadap pihak penyedia jasa TI; dan 3. pihak penyedia jasa TI digunakan sebagai media untuk melakukan rekayasa data BPR atau BPR Syariah dan/atau rekayasa keuangan BPR atau BPR Syariah. |  |
| 1. Dalam hal BPR atau BPR Syariah akan menghentikan penggunaan pihak penyedia jasa TI, BPR atau BPR Syariah wajib: 2. menyusun rencana penghentian penggunaan pihak penyedia jasa TI; 3. memastikan kelangsungan layanan dan data terkait dengan kegiatan yang diserahkan kepada pihak penyedia jasa TI serta kelangsungan kegiatan usaha dan/atau operasional BPR atau BPR Syariah; dan 4. memastikan penghentian penggunaan pihak penyedia jasa TI tidak menimbulkan gangguan pada kegiatan usaha dan/atau operasional BPR atau BPR Syariah. | Ayat (4)  Huruf a  Cukup jelas.  Huruf b  Cukup jelas.  Huruf c  BPR atau BPR Syariah antara lain memastikan bahwa semua data nasabah dan/atau calon nasabah telah dikembalikan atau dimusnahkan oleh pihak penyedia jasa TI. Termasuk dalam kegiatan usaha BPR atau BPR Syariah yaitu layanan kepada nasabah dengan memperhatikan aspek kerahasiaan, integritas, dan ketersediaan data. |  |
| **Pasal 26** | **Pasal 26** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 24 ayat (2), ayat (3), ayat (4), ayat (5), Pasal 25 ayat (1), dan/atau ayat (4) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 24 ayat (2), ayat (3), ayat (4), ayat (5), Pasal 25 ayat (1), dan/atau ayat (4), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 27** | **Pasal 27** |  |
| Ketentuan lebih lanjut mengenai penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI BPR atau BPR Syariah ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB VII** |  |  |
| **PENEMPATAN SISTEM ELEKTRONIK** |  |  |
| **Pasal 28** | **Pasal 28** |  |
| 1. BPR atau BPR Syariah wajib menempatkan Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia. | Ayat (1)  Cukup jelas. |  |
| 1. BPR atau BPR Syariah wajib menempatkan Pusat Data di lokasi dengan karakteristik risiko yang berbeda dengan lokasi Pusat Pemulihan Bencana. | Ayat (2)  Yang dimaksud dengan “karakteristik risiko” antara lain huru-hara dan bencana alam seperti gempa bumi atau banjir. |  |
| **Pasal 29** | **Pasal 29** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 28 dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 28, BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 30** | **Pasal 30** |  |
| Ketentuan lebih lanjut mengenai penempatan Sistem Elektronik ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB VIII** |  |  |
| **PENGELOLAAN DATA DAN PELINDUNGAN DATA PRIBADI DALAM PENYELENGGARAAN TI BPR DAN BPR SYARIAH** |  |  |
| **Bagian Kesatu** |  |  |
| **Pengelolaan Data oleh BPR dan BPR Syariah** |  |  |
| **Pasal 31** | **Pasal 31** |  |
| 1. BPR atau BPR Syariah wajib mengelola data secara efektif dalam pemrosesan data BPR atau BPR Syariah untuk mendukung pencapaian tujuan bisnis BPR atau BPR Syariah. | Ayat (1)  Bentuk pemrosesan data antara lain perolehan, pendistribusian, pengolahan, pemeliharaan, penyimpanan, dan penghapusan data. |  |
| 1. Pengelolaan data secara efektif sebagaimana dimaksud pada ayat (1) memperhatikan paling sedikit: 2. kualitas data; 3. sistem pengelolaan data; dan 4. sumber daya pendukung pengelolaan data. | Ayat (2)  Huruf a  Yang dimaksud dengan “kualitas data” adalah keandalan dan akurasi data.  Huruf b  Sistem pengelolaan data disesuaikan dengan kebutuhan dan kompleksitas BPR atau BPR Syariah.  Sistem pengelolaan data antara lain penyimpanan, penggunaan, dan keamanan data;  Huruf c  Sumber daya pendukung pengelolaan data antara lain berupa infrastruktur TI yang diigunakan untuk mendukung sistem pengelolaan data. |  |
| **Bagian Kedua** |  |  |
| **Pelindungan Data Pribadi oleh BPR dan BPR Syariah** |  |  |
| **Pasal 32** | **Pasal 32** |  |
| 1. BPR atau BPR Syariah wajib melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi sesuai dengan ketentuan peraturan perundang-undangan. | Ayat (1)  Pemrosesan data pribadi antara lain:   1. pemerolehan dan pengumpulan; 2. pengolahan; 3. penyimpanan; 4. transfer atau penyebarluasan; dan/ atau 5. penghapusan atau pemusnahan.   Peraturan perundang-undangan, antara lain:   1. Peraturan perundang-undangan mengenai pelindungan data pribadi; dan 2. Peraturan Otoritas Jasa Keuangan mengenai pelindungan konsumen dan masyarakat di sektor jasa keuangan |  |
| 1. Pemrosesan data pribadi sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan persetujuan nasabah dan/atau calon nasabah yang dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan. | Ayat (2)  Cukup jelas. |  |
| **Pasal 33** | **Pasal 33** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 31 ayat (1) dan/atau Pasal 32 ayat (1) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 31 ayat (1) dan/atau Pasal 32 ayat (1), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 34** | **Pasal 34** |  |
| Ketentuan lebih lanjut mengenai pengelolaan data dan pelindungan data pribadi oleh BPR atau BPR Syariah ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB IX** |  |  |
| **PENGENDALIAN DAN AUDIT INTERN BPR DAN BPR SYARIAH DALAM PENYELENGGARAAN TI BPR DAN BPR SYARIAH** |  |  |
| **Bagian Kesatu** |  |  |
| **Pengendalian Intern BPR atau BPR Syariah dalam Penyelenggaraan TI** |  |  |
| **Pasal 35** | **Pasal 35** |  |
| 1. BPR atau BPR Syariah wajib melaksanakan sistem pengendalian intern secara efektif dalam penyelenggaraan TI. | Ayat (1)  Prinsip umum pelaksanaan sistem pengendalian intern TI dilaksanakan sesuai dengan:   1. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi BPR; atau 2. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi BPR Syariah. |  |
| 1. Pelaksanaan sistem pengendalian intern secara efektif paling sedikit harus mampu mendeteksi kelemahan dan penyimpangan yang terjadi, secara tepat waktu. | Ayat (2)  Cukup jelas. |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud pada ayat (1) dikenai sanksi administratif sesuai dengan: 2. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi BPR; atau 3. Peraturan Otoritas Jasa Keuangan mengenai penerapan manajemen risiko bagi BPR Syariah. | Ayat (3)  Cukup jelas. |  |
| **Bagian Kedua** |  |  |
| **Audit Intern dalam Penyelenggaraan TI** |  |  |
| **Pasal 36** | **Pasal 36** |  |
| 1. BPR dan BPR Syariah wajib melaksanakan audit intern terhadap penyelenggaraan TI sesuai dengan ketentuan peraturan perundang-undangan. | Ayat (1)  Termasuk dalam ketentuan peraturan perundang-undangan antara lain Peraturan Otoritas Jasa Keuangan mengenai penerapan tata kelola bagi BPR dan BPR Syariah. |  |
| 1. BPR dan BPR Syariah wajib melaksanakan audit intern sebagaimana dimaksud pada ayat (1) secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun. | Ayat (2)  Pelaksanaan audit intern dapat dilaksanakan sebagai bagian dari pelaksanaan audit intern atau terpisah dari pelaksanaan audit intern. |  |
| 1. Dalam melaksanakan audit intern sebagaimana dimaksud pada ayat (1), BPR atau BPR Syariah wajib memiliki pedoman audit intern atas penyelenggaraan TI. | Ayat (3)  Penyelenggaraan TI termasuk penyelenggaraan TI BPR atau BPR Syariah oleh pihak penyedia jasa TI. |  |
| 1. Dalam rangka pelaksanaan audit intern sebagaimana dimaksud pada ayat (1), BPR dan BPR Syariah wajib memastikan tersedianya jejak audit (*audit trail*) terhadap seluruh kegiatan penyelenggaraan TI untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya. | Ayat (4)  Yang dimaksud dengan “memastikan tersedianya jejak audit” adalah memastikan tersedianya *log* transaksi dan memelihara *log* tersebut sesuai dengan ketentuan peraturan perundang-undangan dan kebijakan retensi data BPR atau BPR Syariah guna menjamin tersedianya jejak audit yang jelas sehingga dapat digunakan untuk membantu pembuktian dan penyelesaian perselisihan serta pendeteksian usaha penyusupan pada Sistem Elektronik. |  |
| 1. Pelaksanaan audit intern sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh auditor ekstern. | Ayat (5)  Penggunaan auditor ekstern harus mempertimbangkan ukuran dan kompleksitas usaha BPR atau BPR Syariah, serta memperhatikan ketentuan peraturan perundang-undangan terkait auditor ekstern. |  |
| **Pasal 37** | **Pasal 37** |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 36 ayat (1), ayat (2), ayat (3), dan/atau ayat (4) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 36 ayat (1), ayat (2), ayat (3), dan/atau ayat (4), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 38** | **Pasal 38** |  |
| Ketentuan lebih lanjut mengenai pengendalian dan audit intern dalam penyelenggaraan TI BPR atau BPR Syariah ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB X** |  |  |
| **PELAPORAN** |  |  |
| **Bagian Kesatu** |  |  |
| **Laporan Rutin** |  |  |
| **Pasal 39** | **Pasal 39** |  |
| 1. BPR atau BPR Syariah wajib menyampaikan laporan kepada Otoritas Jasa Keuangan mengenai pelaksanaan audit intern sebagaimana dimaksud dalam Pasal 36 ayat (1) sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata ​kelola bagi BPR dan BPR Syariah. | Cukup jelas. |  |
| 1. BPR atau BPR Syariah yang melanggar ketentuan sebagaimana dimaksud pada ayat (1) dikenai sanksi administratif sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai penerapan tata ​kelola bagi BPR dan BPR Syariah. |  |  |
| **Bagian Kedua** |  |  |
| **Laporan Insidentil** |  |  |
| **Pasal 40** | **Pasal 40** |  |
| BPR atau BPR Syariah wajib menyampaikan laporan kepada Otoritas Jasa Keuangan mengenai kondisi terkini penyelenggaraan TI BPR atau BPR Syariah dalam hal terjadi perubahan mendasar dalam penyelenggaraan TI, paling lambat 10 (sepuluh) hari kerja sejak perubahan mendasar dalam penyelenggaraan TI. | Cakupan laporan kondisi terkini penyelenggaraan TI BPR atau BPR Syariah paling sedikit meliputi penjelasan mengenai TI yang diselenggarakan, struktur organisasi yang menggambarkan penyelenggaraan TI, dan kebijakan dan prosedur yang dimiliki terkait penyelenggaraan TI.  Yang dimaksud dengan “perubahan mendasar” antara lain perubahan terhadap konfigurasi TI atau aplikasi inti perbankan, pengadaan aplikasi inti perbankan, kerja sama dengan penyedia jasa TI, serta pengembangan dan pengadaan TI mendasar lainnya yang dapat menambah dan/atau meningkatkan risiko BPR atau BPR Syariah. |  |
| **Pasal 41** | **Pasal 41** |  |
| BPR atau BPR Syariah wajib menyampaikan laporan realisasi penggunaan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 24 ayat (1) paling lambat 10 (sepuluh) hari kerja sejak penyelenggaraan TI BPR atau BPR Syariah oleh penyedia jasa TI efektif beroperasi. | Yang dimaksud dengan “efektif beroperasi” adalah tahapan yang mana TI telah diimplementasikan dan digunakan dalam kegiatan operasional BPR atau BPR Syariah. |  |
| **Pasal 42** | **Pasal 42** |  |
| 1. Dalam hal terjadi insiden TI yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan dan/atau mengganggu kelancaran operasional BPR atau BPR Syariah, BPR atau BPR Syariah wajib menyampaikan: 2. notifikasi awal paling lama 24 (dua puluh empat) jam setelah insiden TI diketahui; dan 3. laporan insiden TI paling lama 7 (tujuh) hari kerja setelah insiden TI diketahui. | Ayat (1)  Insiden TI yaitu kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan TI, berupa:   1. insiden siber; dan 2. insiden nonsiber.   Yang dimaksud kejadian kritis antara lain kegagalan sistem yang serius, *system down time*, dan degradasi kinerja sistem yang mempengaruhi kinerja BPR atau BPR Syariah dalam memberikan pelayanan kepada nasabah.  Insiden siber yaitu ancaman siber, berupa upaya, kegiatan, dan/atau tindakan, yang mengakibatkan Sistem Elektronik tidak berfungsi sebagaimana mestinya.  Contoh insiden siber yaitu tidak berfungsinya Sistem Elektronik sebagaimana mestinya yang disebabkan oleh serangan siber antara lain peretasan, virus, *malware*, *ransomware*, *web defacement*, dan *distributed denial of service attacks*.  Yang dimaksud dengan “kerugian” adalah kerugian keuangan dan/atau kerugian nonkeuangan. Contoh kerugian nonkeuangan yaitu pemberitaan tindakan yang memengaruhi reputasi BPR atau BPR Syariah. |  |
| 1. Notifikasi awal sebagaimana dimaksud pada ayat (1) huruf a disampaikan melalui sarana elektronik secara tertulis kepada Otoritas Jasa Keuangan berdasarkan informasi awal yang tersedia. | Ayat (2)  Notifikasi awal disampaikan kepada satuan kerja pengawasan dari BPR atau BPR Syariah. Contoh sarana elektronik secara tertulis yaitu surat elektronik. |  |
| 1. Dalam hal terdapat pengaturan otoritas lain mengenai penyampaian notifikasi awal dan/atau laporan insiden TI dalam jangka waktu yang lebih cepat daripada jangka waktu sebagaimana dimaksud pada ayat (1), BPR atau BPR Syariah wajib menyampaikan notifikasi awal dan/atau laporan insiden TI kepada Otoritas Jasa Keuangan pada saat yang bersamaan sesuai dengan ketentuan peraturan perundang-undangan otoritas lain dimaksud. | Ayat (3)  Cukup jelas. |  |
| 1. BPR atau BPR Syariah yang telah menyampaikan notifikasi awal dan/atau laporan insiden TI sebagaimana dimaksud pada ayat (3) dianggap telah memenuhi ketentuan sebagaimana dimaksud pada ayat (1) huruf a dan/atau huruf b. | Ayat (4)  Cukup jelas. |  |
| **Bagian Ketiga** |  |  |
| **Tata Cara Penyampaian Laporan** |  |  |
| **Pasal 43** | **Pasal 43** |  |
| 1. BPR atau BPR Syariah menyampaikan laporan: 2. kondisi terkini penyelenggaraan TI sebagaimana dimaksud dalam Pasal 40; 3. laporan realisasi penggunaan pihak penyedia jasa TI sebagaimana dimaksud dalam Pasal 41; dan/atau 4. insiden TI sebagaimana dimaksud dalam Pasal 42 ayat (1) huruf b,   secara daring melalui sistem pelaporan Otoritas Jasa Keuangan. | Cukup jelas. |  |
| 1. BPR atau BPR Syariah yang melakukan pelanggaran terkait penyampaian laporan sebagaimana dimaksud pada ayat (1) dikenai sanksi administratif. |  |  |
| 1. Tata cara penyampaian laporan secara daring sebagaimana dimaksud pada ayat (1) dan pengenaan sanksi administratif sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai pelaporan melalui sistem pelaporan otoritas jasa keuangan dan transparansi kondisi keuangan bagi bank perekonomian rakyat dan bank perekonomian rakyat syariah. |  |  |
| **Pasal 44** | **Pasal 44** |  |
| 1. BPR atau BPR Syariah yang terlambat menyampaikan notifikasi awal insiden TI sebagaimana dimaksud dalam Pasal 42 ayat (1) huruf a atau ayat (3) dikenai sanksi administratif berupa teguran tertulis. | Cukup jelas. |  |
| 1. Dalam hal BPR atau BPR Syariah telah dikenai sanksi administratif sebagaimana dimaksud pada ayat (1) dan belum memenuhi ketentuan sebagaimana dimaksud dalam Pasal 42 ayat (1) huruf a atau ayat (3), BPR atau BPR Syariah dikenai sanksi administratif berupa: 2. pembekuan produk tertentu; 3. larangan untuk menyelenggarakan produk baru; dan/atau 4. penurunan penilaian faktor tata kelola dalam penilaian tingkat kesehatan BPR atau BPR Syariah. |  |  |
| **Pasal 45** | **Pasal 45** |  |
| BPR atau BPR Syariah yang menyampaikan laporan secara tidak lengkap dikenai sanksi administratif atas kesalahan informasi sesuai dengan Peraturan Otoritas Jasa Keuangan mengenai pelaporan melalui sistem pelaporan otoritas jasa keuangan dan transparansi kondisi keuangan bagi bank perekonomian rakyat dan bank perekonomian rakyat syariah. | Cukup jelas. |  |
| **Pasal 46** | **Pasal 46** |  |
| Ketentuan lebih lanjut mengenai format pelaporan dan tata cara penyampaian laporan ditetapkan oleh Otoritas Jasa Keuangan. | Cukup jelas. |  |
|  |  |  |
| **BAB XI** |  |  |
| **KETENTUAN PENUTUP** |  |  |
| **Pasal 47** | **Pasal 47** |  |
| Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku, Peraturan Otoritas Jasa Keuangan Nomor 75/POJK.03/2016 tentang Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 308, Tambahan Lembaran Negara Republik Indonesia Nomor 5998), dicabut dan dinyatakan tidak berlaku. | Cukup jelas. |  |
| **Pasal 48** | **Pasal 48** |  |
| Pada saat Peraturan Otoritas Jasa Keuangan ini mulai berlaku, ketentuan pelaksanaan dari peraturan Otoritas Jasa Keuangan Nomor 75/POJK.03/2016 tentang Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 308, Tambahan Lembaran Negara Republik Indonesia Nomor 5998), dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Peraturan Otoritas Jasa Keuangan ini. | Cukup jelas. |  |
| **Pasal 49** | **Pasal 49** |  |
| Peraturan Otoritas Jasa Keuangan ini mulai berlaku setelah 1 (satu) tahun terhitung sejak tanggal diundangkan. | Cukup jelas. |  |
|  |  |  |
| Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Otoritas Jasa Keuangan ini dengan penempatannya dalam Lembaran Negara Republik Indonesia. |  |  |
|  |  |  |
| Ditetapkan di Jakarta |  |  |
| pada tanggal ... |  |  |
| KETUA DEWAN KOMISIONER OTORITAS JASA KEUANGAN REPUBLIK INDONESIA, |  |  |
| ttd |  |  |
| MAHENDRA SIREGAR |  |  |
|  |  |  |
| Diundangkan di Jakarta |  |  |
| pada tanggal ... |  |  |
| MENTERI HUKUM REPUBLIK INDONESIA, |  |  |
| ttd |  |  |
| SUPRATMAN ANDI AGTAS |  |  |
|  |  |  |