ネットワークデータ安全管理条例

（国務院令第 790 号により 2024 年 9 月 24 日公布、2025 年 1 月 1 日施行）

第 1 章　総則

第 1 条　ネットワークデータ処理活動を規範化し、ネットワークデータ安全を保障し、ネットワークデータの法による合理的・効果的な利用を促進し、個人・組織の適法な権益を保護し、国家の安全及び公共の利益を維持するため、「中華人民共和国ネットワーク安全法」、「中華人民共和国データ安全法」、「中華人民共和国個人情報保護法」等の法律に基づき、本条例を制定する。

第 2 条　中華人民共和国国内において、ネットワークデータ処理活動及びその安全監督管理を展開する際に、本条例を適用する。

中華人民共和国国外において中華人民共和国国内の自然人の個人情報を処理する活動で、「中華人民共和国個人情報保護法」第 3 条第 2 項に定める事由に該当するものについても、本条例を適用する。

中華人民共和国国外において、ネットワークデータ処理活動を展開し、中華人民共和国の国家の安全、公共の利益又は公民・組織の適法な権益を損なう場合には、法により法的責任を追及する。

第 3 条　ネットワークデータ安全管理業務では、中国共産党の指導を堅持し、総体的国家安全観を徹底し、ネットワークデータの開発利用の促進及びネットワークデータ安全の保障を統一的に計画する。

第 4 条　国は、各業界・各領域におけるネットワークデータの革新的応用を奨励し、ネットワークデータ安全防護能力の構築を強化し、ネットワークデータに関連する技術・製品・サービスの革新を支持し、ネットワークデータ安全に係る宣伝教育及び人材育成を展開し、ネットワークデータの開発利用及び産業発展を促進する。

第 5 条　国は、ネットワークデータの経済社会発展における重要度及びひとたび改ざん、破壊、漏洩又は不法取得、不法利用に遭った場合に国家の安全、公共の利益又は個人・組織の適法な権益に対してもたらされる危害の程度に基づき、ネットワークデータに対して分類・分級保護を実行する。

第 6 条　国は、ネットワークデータ安全に関連する国際規則及び標準の制定に積極的に関与し、国際交流及び協力を促進する。

第 7 条　国は、関連する業界組織が規約に従い、ネットワークデータ安全行為規範を制定し、業界自律を強化し、会員を指導してネットワークデータ安全保護を強化させ、ネットワークデータ安全保護水準を向上させ、業界の健全な発展を促進していくことを支持する。

第 2 章　一般規定

第 8 条　いかなる個人・組織も、ネットワークデータを利用して不法活動に従事してはならず、ネットワークデータの窃取又はその他の不法な方式による取得、ネットワークデータの不法販売又は他人への不法提供等の不法なネットワークデータ処理活動に従事してはならない。

いかなる個人・組織も、前項の不法活動への従事に専ら用いられるプログラム及びツールを提供してはならない。他人が前項の不法活動に従事していることを明らかに知っている場合には、その者のためにインターネット接続、サーバーホスティング、ネットワークストレージ、通信伝送等の技術サポートを提供し、又は広告宣伝、支払決済等の幇助をしてはならない。

第 9 条　ネットワークデータ処理者は、法律・行政法規の規定及び国家標準の強制的要求により、ネットワーク安全等級保護の基礎の上において、ネットワークデータ安全防護を強化し、ネットワークデータ安全管理制度を確立して健全化し、暗号化、バックアップ、アクセスコントロール、セキュリティ認証等の技術措置及びその他の必要措施を講じて、改ざん、破壊、漏洩又は不法取得、不法利用に遭わないようにネットワークデータを保護し、ネットワークデータ安全インシデントに対処し、ネットワークデータを対象として、及び利用して実施される違法犯罪活動を防御し、かつ、処理するネットワークデータの安全に対して主体責任を負わなければならない。

第 10 条　ネットワークデータ処理者が提供するネットワーク製品・サービスは、関連する国家標準の強制的要求に適合しなければならない。ネットワーク製品・サービスに安全上の欠陥、脆弱性等のリスクが存在することを発見した場合には、直ちに救済措置を講じ、規定に従って遅滞なくユーザーに告知し、かつ、関係主管部門に報告しなければならない。国家の安全又は公共の利益に対する危害に関わる場合には、ネットワークデータ処理者は、更に、関係主管部門に 24 時間内に報告しなければならない。

第 11 条　ネットワークデータ処理者は、ネットワークデータ安全インシデント緊急時対応計画を確立して健全化しなければならず、ネットワークデータ安全インシデントが発生した場合には、直ちに対応計画を始動させ、措置を講じて危害の拡大を防止し、安全上の潜在的リスクを除去し、かつ、規定に従って関係主管部門に報告しなければならない。

ネットワークデータ安全インシデントが個人・組織の適法な権益に対して危害をもたらす場合には、ネットワークデータ処理者は、安全インシデント及びリスクの状況、危害の結果、既に講じた救済措置等について、電話、ショートメッセージ、インスタントメッセンジャー、電子メール又は公告等の方式をもって、利害関係者に遅滞なく通知しなければならない。通知しないことができる旨を法律・行政法規が規定している場合には、その規定に従う。ネットワークデータ処理者は、ネットワークデータ安全インシデントに対処する過程において違法犯罪の嫌疑のある端緒を発見した場合には、規定に従って公安機関・国家安全機関に届け出、かつ、捜査、調査及び処分業務の展開に協力しなければならない。

第 12 条　ネットワークデータ処理者は、その他のネットワークデータ処理者に対して、個人情報及び重要データを提供し、又はそれらの処理を委託する場合には、処理の目的、方式、範囲及び安全保護義務等をネットワークデータ受領者と契約等を通じて約定し、

かつ、ネットワークデータ受領者による義務の履行状況に対して監督を行わなければならない。その他のネットワークデータ処理者に対して提供又は処理の委託をした個人情報及び重要データの処理状況記録は、最低 3 年保存しなければならない。

ネットワークデータ受領者は、ネットワークデータ安全保護義務を履行し、かつ、約定の目的、方式、範囲等に従って個人情報及び重要データを処理しなければならない。

2 以上のネットワークデータ処理者は、個人情報及び重要データの処理目的及び処理方式を共同で決定する場合には、各自の権利及び義務を約定しなければならない。

第 13 条　ネットワークデータ処理者がネットワークデータ処理活動を展開する場合において、国家の安全に影響し、又は影響する可能性があるときは、国の関係規定に従って国家安全審査を行わなければならない。

第 14 条　ネットワークデータ処理者が合併、分割、解散、破産等の原因によりネットワークデータを移転する必要がある場合には、ネットワークデータ受領者は、ネットワークデータ安全保護義務の履行を継続しなければならない。

第 15 条　国家機関は、他人に委託して電子政務システムを構築・運行・維持させ、政務データを保存・加工させる場合には、国の関係規定に従い厳格な承認手続を経て、受託者のネットワークデータ処理に係る権限、保護責任等を明確にし、受託者によるネットワークデータ安全保護義務の履行を監督しなければならない。

第 16 条　ネットワークデータ処理者は、国家機関若しくは重要な情報インフラ運営者にサービスを提供し、又はその他の公共インフラ若しくは公共サービスシステムの構築・運行・維持に関与する場合には、法律・法規の規定及び契約の約定によりネットワークデータ安全保護義務を履行し、安全、安定かつ継続的なサービスを提供しなければならない。

前項に定めるネットワークデータ処理者は、委託者の同意を経ていない場合には、ネットワークデータについてアクセス、取得、保管、使用、漏洩又は他人への提供をしてはならず、ネットワークデータに対してアソシエーション分析を行ってはならない。

第 17 条　国家機関にサービスを提供する情報システムは、電子政務システムの管理要求を参照してネットワークデータ安全管理を強化し、ネットワークデータ安全を保障しなければならない。

第 18 条　ネットワークデータ処理者は、自動化ツールを使用してネットワークデータに対しアクセス又は収集をする場合には、ネットワークサービスに与える影響を評価しなければならず、他人のネットワークに不法侵入してはならず、ネットワークサービスの正常な運行に干渉してはならない。

第 19 条　生成系人工知能サービスを提供するネットワークデータ処理者は、トレーニングデータ及びトレーニングデータ処理活動に対する安全管理を強化し、有効な措置を講じてネットワークデータ安全リスクを防御し、及びこれに対処しなければならない。

第 20 条　社会に向けて製品・サービスを提供するネットワークデータ処理者は、社会の監督を受け入れ、ネットワークデータ安全に係る簡便な苦情申立・通報ルートを確立し、苦情申立・通報の方式等の情報を公布し、ネットワークデータ安全に係る苦情申立・通報を遅滞なく受理し、かつ、処理しなければならない。

第 3 章　個人情報保護

第 21 条　ネットワークデータ処理者が個人情報を処理する前において、個人情報処理規則を制定するという方式を通じて法により個人に告知をする場合には、個人情報処理規則は、まとめて公開・表示し、アクセスが容易で、かつ、目立つ位置に置かれ、内容が明確かつ具体的、明瞭で分かりやすく、次の各号に掲げる内容をそれらに限定することなく含むものでなければならない。

（一）　ネットワークデータ処理者の名称又は氏名及び連絡先

（二）　個人情報を処理する目的、方式及び種類、並びに機微な個人情報を処理する必要性及び個人の権益に対する影響

（三）　個人情報の保存期間及び期限到来後の処理方式。保存期間について確定が困難である場合には、保存期間の確定方法を明確にしなければならない。

（四）　個人が個人情報の閲覧、複製、移転、訂正、補足、削除、処理制限をする場合並びにアカウント抹消及び同意撤回をする場合の方法及びルート等

ネットワークデータ処理者は、個人情報の収集及びその他のネットワークデータ処理者への提供の目的、方式及び種類並びにネットワークデータ受領者の情報を前項の規定に従って個人に告知する場合には、リスト等の形式をもって明記しなければならない。ネットワークデータ処理者は、14 歳に満たない未成年者の個人情報を処理する場合には、専門の個人情報処理規則を更に制定しなければならない。

第 22 条　ネットワークデータ処理者は、個人の同意に基づいて個人情報を処理する場合には、次の各号に掲げる規定を遵守しなければならない。

（一）　個人情報の収集が製品又はサービスを提供するために必要である場合には、範囲を逸脱して個人情報を収集してはならず、誤導、詐欺、強迫等の方式を通じて個人の同意を取得してはならない。

（二）　生体識別、宗教信仰、特定の身分、医療健康、金融口座、移動軌跡等の機微な個人情報を処理する場合には、個人の単独の同意を取得しなければならない。

（三）　14 歳に満たない未成年者の個人情報を処理する場合には、未成年者の父母その他の保護者の同意を取得しなければならない。

（四）　個人が同意した個人情報処理に係る目的、方式、種類及び保存期間を逸脱して個人情報を処理してはならない。

（五）　個人がその個人情報の処理に同意しない旨を明確に表明した後に、頻繁に同意を求めてはならない。

（六）　個人情報の処理に係る目的、方式又は種類に変更が生じた場合には、個人の同意を新たに取得しなければならない。

機微な個人情報を処理する場合には書面による同意を取得しなければならない旨を法律・行政法規が規定している場合には、その規定に従う。

第 23 条　個人が自身の個人情報の閲覧、複製、訂正、補足、削除若しくは処理制限を請求し、又は個人がアカウントを抹消し、若しくは同意を撤回する場合には、ネットワークデータ処理者は、遅滞なく受理し、かつ、個人による権利行使に対応する簡便な方法及びルートを提供しなければならず、不合理な条件を設けて個人の合理的な請求を制限してはならない。

第 24 条　自動化収集技術等の使用により、不必要な個人情報又は個人の同意を法どおりに

取得していない個人情報を収集してしまうことを回避する手立てがない場合、及び個人がアカウントを抹消した場合には、ネットワークデータ処理者は、個人情報を削除し、又は匿名化処理を行わなければならない。法律・行政法規で定める保存期間が満了せず、又は個人情報の削除及び匿名化処理が技術的に実現困難な場合には、ネットワークデータ処理者は、保存及び必要な安全保護措置の採用以外の処理を停止しなければならない。

第 25 条　次の各号に掲げる条件に適合する個人情報移転請求に対し、ネットワークデータ処理者は、個人が指定するその他のネットワークデータ処理者による関係個人情報に対するアクセス及び取得のためにルートを提供しなければならない。

（一）　請求者の真実の身分を検証することができること。

（二）　移転が請求されているのが、本人が提供に同意した、又は契約に基づき収集した個人情報であること。

（三）　個人情報の移転が技術的な実行可能性を備えていること。

（四）　個人情報の移転が他人の適法な権益を損なわないこと。

個人情報の移転の請求回数等が合理的な範囲を明らかに逸脱している場合には、ネットワークデータ処理者は、個人情報移転に係るコストに基づき必要費用を徴収することができる。

第 26 条　中華人民共和国国外のネットワークデータ処理者は、国内自然人の個人情報を処理する場合に、「中華人民共和国個人情報保護法」第 53 条の規定により国内において専門機構を設立し、又は代表を指定するときは、関係機構の名称又は代表の氏名、連絡先等を、所在地の区を設置した市級のネット情報部門に提出しなければならず、ネット情報部門は同級の関係主管部門にこれを遅滞なく周知しなければならない。

第 27 条　ネットワークデータ処理者は、自ら又は専門機構に委託して、自身が個人情報を処理する際の法律・行政法規遵守状況に対し、コンプライアンス監査を定期的に行わなければならない。

第 28 条　ネットワークデータ処理者は、1000 万人分以上の個人情報を処理する場合には、重要データを処理するネットワークデータ処理者（以下、重要データの処理者という。）に対して定められた本条例第 30 条及び第 32 条の規定を更に遵守しなければならない。

第 4 章　重要データの安全

第 29 条　国のデータ安全業務調整体制は、関係部門が重要データリストを制定し、重要データに対する保護を強化するよう統一的に計画・調整する。各地区・各部門は、データ分類・分級保護制度に従って当該地区・当該部門及び関連業界・領域の重要データの具体的リストを確定し、リストに組み入れたネットワークデータについては重点的な保護を行わなければならない。

ネットワークデータ処理者は、国の関係規定に従って重要データを識別及び申告しなければならない。重要データと認めるものについて、関連の地区・部門は、遅滞なくネットワークデータ処理者に告知し、又は公開発布しなければならない。ネットワークデータ処理者は、ネットワークデータ安全保護責任を履行しなければならない。

国は、ネットワークデータ処理者がデータのラベリング識別等の技術及び製品を使用し、重要データの安全管理レベルを向上させることを奨励する。

第 30 条　重要データの処理者は、ネットワークデータ安全責任者及びネットワークデータ安全管理機構を明確にしなければならない。ネットワークデータ安全管理機構は、次の各号に掲げるネットワークデータ安全保護責任を履行しなければならない。

（一）　ネットワークデータ安全管理制度、操作規程及びネットワークデータ安全インシデント緊急時対応計画を制定して実施する。

（二）　ネットワークデータ安全に係るリスクモニタリング、リスク評価、緊急時訓練、宣伝教育研修等の活動を定期的に組織・展開し、ネットワークデータ安全に係るリスク及びインシデントに遅滞なく対処する。

（三）　ネットワークデータ安全に係る苦情申立・通報を受理し、かつ、処理する。

ネットワークデータ安全責任者は、ネットワークデータ安全の専門知識及び関連の管理業務経験が備わっていなければならず、ネットワークデータ処理者の経営陣構成員が担当し、関係主管部門にネットワークデータ安全状況を直接報告する権限を有する。

関係主管部門が規定する特定の種類・規模の重要データを把握しているネットワークデータ処理者は、ネットワークデータ安全責任者及び重要部署の人員に対し安全背景審査を行い、関連人員研修を強化しなければならない。審査の際には、公安機関・国家安全機関に協力を申請することができる。

第 31 条　重要データの処理者が重要データを提供、委託処理又は共同処理する前には、リスク評価を行わなければならない。但し、法定の職責又は法定の義務の履行に該当する場合を除く。

リスク評価では、次の各号に掲げる内容を重点的に評価しなければならない。

（一）　ネットワークデータの提供、委託処理又は共同処理、及びネットワークデータ受領者によるネットワークデータ処理の目的、方式、範囲等が適法・正当・必要か否か

（二）　提供、委託処理又は共同処理するネットワークデータが改ざん、破壊、漏洩又は不法取得、不法利用に遭うリスク、及び国家の安全、公共の利益又は個人・組織の適法な権益に対してもたらすリスク

（三）　ネットワークデータ受領者の信義誠実、法令遵守等の状況

（四）　ネットワークデータ受領者と締結した、又は締結しようとしている関連契約中のネットワークデータ安全に関する要求で、ネットワークデータ受領者がネットワークデータ安全保護義務を履行するよう有効に拘束することができるか否か

（五）　採用した、又は採用しようとしている技術及び管理措置等で、ネットワークデータが改ざん、破壊、漏洩又は不法取得、不法利用等に遭うリスクを有効に防御することができるか否か

（六）　関係主管部門が定めるその他の評価内容

第 32 条　重要データの処理者は、合併、分割、解散、破産等により重要データの安全に影響する可能性がある場合には、措置を講じてネットワークデータ安全を保障し、かつ、省級以上の関係主管部門に重要データ取扱案、受領者の名称又は氏名及び連絡先等を報告しなければならない。主管部門が明確でない場合には、省級以上のデータ安全業務調整体制に報告しなければならない。

第 33 条　重要データの処理者は年度毎にそのネットワークデータ処理活動についてリスク評価を展開し、かつ、省級以上の関係主管部門にリスク評価報告を送付しなければなら

ず、関係主管部門は同級のネット情報部門及び公安機関にこれを遅滞なく周知しなければならない。

リスク評価報告には、次の各号に掲げる内容を含まなければならない。

（一）ネットワークデータ処理者の基本情報、ネットワークデータ安全管理機構の情報、ネットワークデータ安全責任者の氏名及び連絡先等

（二）重要データを処理する目的、種類、数量、方式、範囲、保存期間、保存場所等、ネットワークデータ処理活動の展開状況。ネットワークデータの内容自体は含まない。

（三）ネットワークデータ安全管理制度及び実施状況、暗号化、バックアップ、ラベリング識別、アクセスコントロール、セキュリティ認証等の技術措置及びその他の必要措置並びにそれらの有効性

（四）発見されたネットワークデータ安全リスク、発生したネットワークデータ安全インシデント及び対処状況

（五）重要データの提供、委託処理又は共同処理に係るリスク評価状況

（六）ネットワークデータの国外移転状況

（七）関係主管部門が定めるその他の報告内容

重要データを処理する大型ネットワークプラットフォームサービス提供者が送付するリスク評価報告では、前項に定める内容を含むほか、更に基幹業務及びサプライチェーンに係るネットワークデータ安全等の状況を十分に説明しなければならない。

重要データの処理者に、国家の安全を害する可能性のある重要データ処理活動が存在する場合には、省級以上の関係主管部門は、是正又は重要データの処理停止等の措置を講じるようその者に命じなければならない。重要データの処理者は、関係する要求に従って直ちに措置を講じなければならない。

第 5 章　ネットワークデータの越境安全管理

第 34 条　国のネット情報部門は、関係部門が国のデータ国外移転安全管理に係る専門業務体制を確立するよう統一的に計画・調整し、国のネットワークデータ国外移転安全管理に関連する政策について制定に向け検討し、ネットワークデータ国外移転安全に係る重大事項を調整・処理する。

第 35 条　次の各号に掲げる条件のいずれかに適合する場合には、ネットワークデータ処理者は、個人情報を国外に提供することができる。

（一）国のネット情報部門が組織するデータ国外移転安全評価を通過している。

（二）国のネット情報部門の規定に従い、専門機構が行う個人情報保護認証を経ている。

（三）国のネット情報部門が制定した個人情報国外移転標準契約に関する規定に適合している。

（四）個人が一方当事者である契約の締結又は履行のために、個人情報を国外に提供する必要が確かにある。

（五）法により制定された労働規則制度及び法により締結された集団契約に従って越境人的資源管理を実施する際に、従業員の個人情報を国外に提供する必要が確かにある。

（六）　法定の職責又は法定の義務の履行のために、個人情報を国外に提供する必要が確かにある。

（七）　緊急の状況において自然人の生命、健康及び財産の安全を保護するために、個人情報を国外に提供する必要が確かにある。

（八）　法律・行政法規又は国のネット情報部門が定めるその他の条件

第 36 条　中華人民共和国が締結又は参加する国際条約・協定に、中華人民共和国国外に対する個人情報提供の条件等について規定がある場合には、その規定に従って執行することができる。

第 37 条　ネットワークデータ処理者が中華人民共和国国内の運営において収集及び生成した重要データについて、国外に提供する必要が確かにある場合には、国のネット情報部門が組織するデータ国外移転安全評価を通過しなければならない。ネットワークデータ処理者は、国の関係規定に従って重要データを識別及び申告するが、関連の地区・部門によって重要データである旨が告知又は公開発布されていない場合には、それを重要データとしてデータ国外移転安全評価を申告する必要はない。

第 38 条　データ国外移転安全評価を通過した後、ネットワークデータ処理者は、個人情報及び重要データを国外に提供する場合には、評価時に明確にしたデータ国外移転の目的、方式、範囲及び種類、規模等を逸脱してはならない。

第 39 条　国は、措置を講じて、ネットワークデータ越境安全上のリスク及び脅威を防御し、及びこれらに対処する。いかなる個人・組織も、技術措置の破壊又は回避に専ら用いられるプログラム、ツール等を提供してはならない。他人が技術措施の破壊、回避等の活動に従事していることを明らかに知っている場合には、その者のために技術サポート又は幇助をしてはならない。

第 6 章　ネットワークプラットフォームサービス提供者の義務

第 40 条　ネットワークプラットフォームサービス提供者は、プラットフォーム規則又は契約等を通じて、そのプラットフォームに接続する第三者製品・サービス提供者のネットワークデータ安全保護義務を明確にし、第三者製品・サービス提供者がネットワークデータ安全管理を強化するよう督促しなければならない。

アプリケーションプログラムをプリインストールしているスマート端末等デバイス生産者には、前項の規定を適用する。

第三者製品・サービス提供者が法律・行政法規の規定又はプラットフォーム規則若しくは契約の約定に違反してネットワークデータ処理活動を展開し、ユーザーに対して損害を与えた場合には、ネットワークプラットフォームサービス提供者、第三者製品・サービス提供者及びアプリケーションプログラムをプリインストールしているスマート端末等デバイス生産者は、法により相応の責任を負わなければならない。

国は、保険会社がネットワークデータ損害賠償責任に係る保険の種類を開発することを奨励し、ネットワークプラットフォームサービス提供者及びアプリケーションプログラムをプリインストールしているスマート端末等デバイス生産者が保険に加入することを奨励する。

第 41 条　アプリケーションプログラム配信サービスを提供するネットワークプラットフォ

ームサービス提供者は、アプリケーションプログラム確認規則を確立し、かつ、ネットワークデータ安全に関連する確認を展開しなければならない。配信予定又は配信済みのアプリケーションプログラムが法律・行政法規の規定又は国家標準の強制的要求に適合しないことを発見した場合には、警告、配信の取りやめ、配信の一時停止又は配信の終了等の措置を講じなければならない。

第 42 条　ネットワークプラットフォームサービス提供者は、自動化された意思決定方式を通じて個人に情報配信を行う場合には、理解が容易であってアクセス及び操作しやすい、パーソナライズドレコメンドのオフの選択肢を設け、配信情報の受領拒否、その個人的な特徴に焦点を定めたユーザーラベルの削除等の機能をユーザーに提供しなければならない。

第 43 条　国は、ネットワーク身分認証公共サービスの構築を推進し、政府の手引き及びユーザーの自由意思という原則に従って普及応用を行う。

ユーザーが国のネットワーク身分認証公共サービスを使用して真実の身分情報の登録及び確認をすることに、ネットワークプラットフォームサービス提供者が対応していくことは、これを奨励する。

第 44 条　大型ネットワークプラットフォームサービス提供者は、年度毎に個人情報保護に係る社会的責任報告を発布しなければならない。報告内容には、個人情報保護措置及び成果、個人の権利行使に係る申請受理状況、主に外部の構成員により組織される個人情報保護監督機構の職責履行状況等を含むがそれらに限られない。

第 45 条　大型ネットワークプラットフォームサービス提供者は、ネットワークデータを越境提供する場合には、国のデータ越境安全管理要求を遵守し、関連の技術及び管理措置を健全化し、ネットワークデータ越境安全リスクを防御しなければならない。

第 46 条　大型ネットワークプラットフォームサービス提供者は、ネットワークデータ、アルゴリズム及びプラットフォーム規則等を利用し、次の各号に掲げる活動に従事してはならない。

（一）　ユーザーがプラットフォーム上で生成したネットワークデータを誤導、詐欺、強迫等の方式を通じて処理する。

（二）　ユーザーがプラットフォーム上で生成したネットワークデータに対するユーザー自身によるアクセス及び使用を正当な理由なく制限する。

（三）　ユーザーに対して不合理な差をつけた待遇を実施し、ユーザーの適法な権益を損なう。

（四）　法律・行政法規が禁止するその他の活動

第 7 章　監督管理

第 47 条　国のネット情報部門は、ネットワークデータ安全及び関連する監督管理業務の統一的な計画・調整に責任を負う。

公安機関・国家安全機関は、関係する法律・行政法規及び本条例の規定により、各自の職責の範囲内においてネットワークデータ安全監督管理の職責を担い、ネットワークデータ安全を害する違法犯罪活動を法により防御し、及び取り締まる。

国のデータ管理部門は、データ管理業務を具体的に担う中で、相応のネットワークデ

ータ安全の職責を履行する。

各地区・各部門は、当該地区・当該部門の業務において収集及び生成したネットワークデータ及びネットワークデータ安全について責任を負う。

第 48 条　各関係主管部門は、当該業界・当該領域のネットワークデータ安全監督管理の職責を担い、当該業界・当該領域のネットワークデータ安全保護業務機構を明確にし、当該業界・当該領域のネットワークデータ安全インシデント緊急時対応計画を統一的に制定し、かつ、組織・実施し、当該業界・当該領域のネットワークデータ安全リスク評価を定期的に組織・展開し、ネットワークデータ処理者によるネットワークデータ安全保護義務の履行状況に対して監督検査を行い、存在する潜在的リスクに対しネットワークデータ処理者が遅滞なく是正を行うよう指導・督促しなければならない。

第 49 条　国のネット情報部門は、関係主管部門がネットワークデータ安全リスクに関連する情報を遅滞なく集約、検討・評価、共有及び発表し、ネットワークデータ安全に係る情報共有、ネットワークデータ安全上のリスク及び脅威に係るモニタリング・早期警戒並びにネットワークデータ安全インシデント応急対処業務を強化するよう統一的に計画・調整する。

第 50 条　関係主管部門は、次の各号に掲げる措置を講じて、ネットワークデータ安全に対し監督検査を行うことができる。

（一）　監督検査事項について説明を行うようネットワークデータ処理者及びその関連人員に要求する。

（二）　ネットワークデータ安全と関係する文書及び記録を閲覧及び複製する。

（三）　ネットワークデータ安全措置の運行状況を検査する。

（四）　ネットワークデータ処理活動と関係する設備及び物品を検査する。

（五）　法律・行政法規が定めるその他の必要措置

ネットワークデータ処理者は、関係主管部門が法により展開するネットワークデータ安全監督検査に対して協力をしなければならない。

第 51 条　関係主管部門は、ネットワークデータ安全監督検査を展開する場合には、客観的・公正でなければならず、被検査単位から費用を徴収してはならない。

関係主管部門は、ネットワークデータ安全監督検査中に、ネットワークデータ安全と関係のない業務情報に対し、アクセス及び収集をしてはならず、取得した情報は、ネットワークデータ安全の維持に係る必要にのみ用いることができ、その他の用途に用いてはならない。

関係主管部門は、ネットワークデータ処理者のネットワークデータ処理活動に比較的大きい安全リスクが存在することを発見した場合には、ネットワークデータ処理者に対し、関連サービスの一時停止、プラットフォーム規則の修正、技術措置の完全化等をしてネットワークデータ安全上の潜在的リスクを除去するよう、規定された権限及び手続に従って要求することができる。

第 52 条　関係主管部門は、ネットワークデータ安全監督検査を展開する際において、協働・協力及び情報交流を強化し、検査頻度及び検査方式を合理的に確定して、不要な検査及び交差・重複検査を回避しなければならない。

個人情報保護コンプライアンス監査、重要データリスク評価、重要データ国外移転安全評価等は、連携を強化し、重複評価・監査を回避しなければならない。重要データリ

スク評価とネットワーク安全等級測定評価の内容に重複がある場合には、関連の結果は、互いに信用に足るとして採用することができる。

第 53 条　関係主管部門及びその職員は、職責履行中に知った個人のプライバシー、個人情報、商業秘密、秘密保持商務情報等のネットワークデータについて、法により秘密を保持しなければならず、漏洩又は他人への不法な提供をしてはならない。

第 54 条　国外の組織・個人が中華人民共和国の国家の安全若しくは公共の利益を害し、又は中華人民共和国の公民の個人情報に係る権益を侵害するネットワークデータ処理活動に従事した場合には、国のネット情報部門は、関係主管部門と共同して法により相応の必要措置を講じることができる。

第 8 章　法的責任

第 55 条　本条例第 12 条、第 16 条から第 20 条まで、第 22 条、第 40 条第 1 項及び第 2 項、第 41 条並びに第 42 条の規定に違反する場合には、ネット情報、電信、公安等の主管部門が各自の職責により是正を命じ、警告を行い、違法所得を没収する。是正を拒絶し、又は情状が重大である場合には、100 万元以下の過料を科し、かつ、関連業務の一時停止、営業停止・整理、関連業務許可証の取消し又は営業許可証の取消しを命じることができ、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科すことができる。

第 56 条　本条例第 13 条の規定に違反する場合には、ネット情報、電信、公安、国家安全等の主管部門が各自の職責により是正を命じ、警告を行い、併せて 10 万元以上 100 万元以下の過料を科すことができ、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科すことができる。是正を拒絶し、又は情状が重大である場合には、100 万元以上 1000 万元以下の過料を科し、かつ、関連業務の一時停止、営業停止・整理、関連業務許可証の取消し又は営業許可証の取消しを命じることができ、直接責任を負う主管者及びその他の直接責任者に対して 10 万元以上 100 万元以下の過料を科す。

第 57 条　本条例第 29 条第 2 項、第 30 条第 2 項及び第 3 項、第 31 条並びに第 32 条の規定に違反する場合には、ネット情報、電信、公安等の主管部門が各自の職責により是正を命じ、警告を行い、併せて 5 万元以上 50 万元以下の過料を科すことができ、直接責任を負う主管者及びその他の直接責任者に対して 1 万元以上 10 万元以下の過料を科すことができる。是正を拒絶し、又は大量データ漏洩等の重大な結果をもたらした場合には、50 万元以上 200 万元以下の過料を科し、かつ、関連業務の一時停止、営業停止・整理、関連業務許可証の取消し又は営業許可証の取消しを命じることができ、直接責任を負う主管者及びその他の直接責任者に対して 5 万元以上 20 万元以下の過料を科す。

第 58 条　本条例のその他の関係規定に違反する場合には、関係主管部門が「中華人民共和国ネットワーク安全法」、「中華人民共和国データ安全法」、「中華人民共和国個人情報保護法」等の法律の関係規定により法的責任を追及する。

第 59 条　ネットワークデータ処理者で、違法行為による危害の結果を自ら進んで除去若しくは軽減している、違法行為が軽微であって遅滞なく是正しており危害の結果をもたらしていない、又は初めて法に違反し危害の結果が軽微であって遅滞なく是正している等

の事由が存在するものについては、「中華人民共和国行政処罰法」の規定により、軽きに従って行政処罰し、行政処罰を減軽し、又は行政処罰をしない。

第 60 条　国家機関が本条例に定めるネットワークデータ安全保護義務を履行しない場合には、その上級機関又は関係主管部門が是正を命じる。直接責任を負う主管者及びその他の直接責任者に対しては、法によりこれを処分する。

第 61 条　本条例の規定に違反し、他人に損害をもたらした場合には、法により民事責任を負う。治安管理違反行為を構成する場合には、法により治安管理処罰をする。犯罪を構成する場合には、法により刑事責任を追及する。

第 9 章　附則

第 62 条　本条例において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（一）　ネットワークデータとは、ネットワークを通じて処理及び生成される各種電子データをいう。

（二）　ネットワークデータ処理活動とは、ネットワークデータの収集、保存、使用、加工、送信、提供、公開、削除等の活動をいう。

（三）　ネットワークデータ処理者とは、ネットワークデータ処理活動において、処理目的及び処理方式を自主的に決定する個人・組織をいう。

（四）　重要データとは、特定の領域、特定の集団若しくは特定の区域の、又は一定の精度及び規模に達し、ひとたび改ざん、破壊、漏洩又は不法取得、不法利用に遭った場合に国家の安全、経済の運営、社会の安定並びに公共の健康及び安全を直接害する可能性のあるデータをいう。

（五）　委託処理とは、ネットワークデータ処理者が個人・組織に委託し、約定の目的及び方式に従って展開させるネットワークデータ処理活動をいう。

（六）　共同処理とは、2 以上のネットワークデータ処理者がネットワークデータの処理目的及び処理方式を共同で決定するネットワークデータ処理活動をいう。

（七）　単独の同意とは、自身の個人情報に特定の処理が行われることに対して個人が個別になした具体的かつ明確な同意をいう。

（八）　大型ネットワークプラットフォームとは、登録ユーザーが 5000 万以上又は月間アクティブユーザーが 1000 万以上の、業務類型が複雑であり、ネットワークデータ処理活動が国家の安全、経済の運営、国家経済・国民生活等に対し重要な影響を有するネットワークプラットフォームをいう。

第 63 条　核心データのネットワークデータ処理活動を展開する場合には、国の関係規定に従って執行する。

自然人が個人又は家庭の事務を理由に個人情報を処理する場合には、本条例を適用しない。

国家秘密又は業務秘密に関わるネットワークデータ処理活動を展開する場合には、「中華人民共和国国家秘密保護法」等の法律・行政法規の規定を適用する。

第 64 条　本条例は、2025 年 1 月 1 日から施行する。

（法令原文名称：网络数据安全管理条例）