



LexisNexis® Data Privacy Policy

The LexisNexis Data Privacy Policy covers personally identifiable information received by LexisNexis, a division of Reed Elsevier, Inc. from its data suppliers, and which is distributed on the LexisNexis services. This personally identifiable information is contained in public records, publicly available information and non-public information (see definitions below). The LexisNexis Data Privacy Policy does not cover information that may be collected by LexisNexis from the user, whether online or offline. The LexisNexis Website Privacy Policy titled, "Privacy Notice – Your Privacy is Important to Us," governs the collection of information from users of LexisNexis websites. See <http://www.lexisnexis.com/terms/privacy/>.

LexisNexis is committed to promoting the responsible use of information and protecting individual privacy rights. In recognition of this commitment, LexisNexis adheres to the principles contained within its data privacy policy. LexisNexis recognizes that statutes such as the Driver's Privacy Protection Act (federal and state) and the Gramm-Leach-Bliley Act regulate some of the personally identifiable information distributed on the LexisNexis services. LexisNexis diligently complies with the requirements of these laws.

LexisNexis reserves the right to deviate from this Data Privacy Policy if it is required to do so by operation of law, upon request of law enforcement, or, if necessary, to prevent fraud or to maintain integrity of its computer systems.

1. DEFINITIONS.

Personally Identifiable Information

Personally identifiable information means information about a specific individual that either identifies the individual or is directly attributed to the individual. Personally identifiable information is contained in public records, non-public information and publicly available information. Examples of personally identifiable information include:

- Name;
- Address;
- Date of birth; and
- Telephone number.

Public Records

Public records are those records created and maintained by government agencies and are open for public inspection. Examples of public records include:

- Real-estate title records;
- Judgments and liens;
- Bankruptcy records;
- Motor-vehicle registrations; and
- Uniform Commercial Code (UCC) filings.

Non-Public Information

Non-public information is information about an individual obtained from a source that is privately owned and is not available to the general public. Non-public information may include the following data elements:

- Name;
- Current and previous addresses;
- Social Security number (for LexisNexis' policy on the distribution of Social Security numbers see Principle 6 below);
- Previous names used, such as alias names, maiden names or previous married names; and
- Birth date information.

Publicly Available Information

Publicly Available Information is information about an individual that is available to the general public from non-governmental sources. Sources of publicly available information include:

- Newspapers and other publications;
- Telephone directories; and
- Magazines.

Appropriate or Appropriately

Describes actions or uses that are reasonable under the circumstances reflecting a balance between the interests of individual privacy and legitimate business, governmental, and professional uses of personally identifiable information, including but not limited to:

- Prevention and detection of fraud;
- Investigation of criminal activity;
- Litigation support; and
- Enforcement of judgments.

2. EDUCATION – LexisNexis informs its employees, users and the general public about appropriate use of its products and services.

LexisNexis informs its users and employees about:

- Privacy issues associated with LexisNexis' information products and services;
- The responsible use of public records, publicly available information and non-public information; and
- The societal benefits arising from the free flow of information.

LexisNexis informs the public about:

- Privacy issues associated with LexisNexis' information products and services;
- Measures LexisNexis has undertaken to enhance consumer privacy;
- Choices available to consumers regarding information access and the ability to opt-out of its products and services containing non-public information products; and
- How consumers benefit from the responsible flow of information.

3. REPUTABLE SOURCES - LexisNexis acquires public records and non-public information from established, reputable sources in the government and private sectors.

LexisNexis acquires public records and non-public information from established, reputable sources in the government and private sectors. Reasonable steps will be taken to:

- Review the supplier's data collection practices and policies;
- Review the supplier's business practices;
- Review the financial condition of the supplier; and
- Review the types of data the supplier sells (public record, publicly available or non-public information).

LexisNexis obtains an assurance from each data supplier that the supplier has the legal right to license or sell the data to LexisNexis.

4. ACCURACY – LEXISNEXIS endeavors to accurately reproduce all information in its products.

While maintaining, using or disseminating personally identifiable information LexisNexis takes reasonable steps to accurately reproduce data it receives from its suppliers. However, due to the nature of public records, non-public information or publicly available information, it is reasonable to expect these files to contain some errors. If a record is suspected to be inaccurate, refer to Principle 10 on Access and Correctability.

For non-public information, LexisNexis will, for a nominal fee, provide individuals with copies of non-public information about themselves contained in applicable products and services to verify the accuracy of that information. For public records and publicly available information, LexisNexis will direct the consumer to the data supplier or government entity that can review the claim of inaccuracy and make appropriate corrections.

5. DISTRIBUTION OF NON-PUBLIC INFORMATION – LexisNexis distributes non-public information only to LexisNexis users.

LexisNexis distributes non-public information only to its users and not to the public in general. Typical LexisNexis users of non-public information include law firms, government agencies, law enforcement personnel, and other commercial and professional users. Users generally use non-public information to locate individuals and verify information provided to them by the individuals.

If upon investigation LexisNexis finds that non-public information is used inappropriately or unlawfully, LexisNexis will take reasonable steps to stop the misuse, educate the user concerning the appropriate and lawful use of the information, and to prevent similar future misuses. In the event of repeated misuse, LexisNexis may discontinue a user's access to LexisNexis information products and services.

LexisNexis does not collect, maintain, or distribute personal financial information such as bank account numbers and balances, credit card account information, personal information on individuals known to be minors, or mother's maiden names designated as such in non-public information files distributed as part of LexisNexis' online services.

6. DISTRIBUTION OF SOCIAL SECURITY NUMBERS AND DRIVER'S LICENSE NUMBERS – LexisNexis limits the availability of Social Security and Driver's License numbers.

Except as otherwise provided herein, a user cannot access fully displayed Social Security numbers (SSNs) from non-public information files or Driver's License Numbers (DLNs) obtained directly or indirectly from government agencies that issue driver's licenses. Users may search records using a SSN or a DLN in their possession but records retrieved will not display the full SSN or DLN.

For SSNs, users will receive SSNs with the last four characters truncated in their search results. An example of a truncated SSN is 123-45-XXXX. For Driver's license records, the DLN will not display.

LexisNexis displays full SSNs and DLNs to the following group of pre-qualified users:

- State, local and federal government entities with law enforcement responsibilities;
- Special investigative units (SIUs) and subrogation and claims departments of public or private insurance companies for the purposes of detecting, investigating or preventing fraud;
- Departments within financial institutions for the purpose of detecting, investigating or preventing fraud, for compliance with state and federal laws and regulations, and for the purpose of collecting debt on their own behalf;
- Collection departments of a creditor, collection departments of law firms, and collection companies acting on behalf of a creditor or on their own behalf; and
- Other public or private entities, on a case-by-case basis, for the purposes of detecting, investigating or preventing fraud or other criminal activities, or enforcing legal rights or remedies.

LexisNexis displays SSNs and DLNs to the pre-qualified users for the following types of authorized uses:

- Location or investigation of suspects, witnesses or criminals;
- Location of non-custodial spouses allegedly owing child support or ex-spouses allegedly owing spousal support;
- Location of individuals alleged to have failed to pay taxes or other lawful debts;
- Verification of identity; or
- Other uses similar to those described above with prior review and approval by LexisNexis.

LexisNexis does not provide SSNs from non-public information files or DLNs obtained directly or indirectly from government agencies that issue driver's licenses to the general public or to users other than the pre-qualified users described above.

LexisNexis provides verification tools to its users that will correct two mis-keyed digits in a SSN where the user provides the SSN and other required data elements.

A limited number of public records may contain SSNs. This principle does not apply to the display of SSNs found in public records.

7. SECURITY – LEXISNEXIS endeavors to keep its data secure.

LexisNexis undertakes reasonable steps to maintain facilities and systems to protect personally identifiable information from unauthorized access or access by persons who attempt to exceed their authorization.

8. NOTICE – LEXISNEXIS makes its Data Privacy Policy publicly known.

LexisNexis publicly posts this Data Privacy Policy, which include the following key principles on its website, <http://www.lexisnexis.com/terms/privacy/data/>:

1. Definitions;
2. Education;
3. Reputable Sources;
4. Accuracy;
5. Distribution of Non-Public Information;
6. Distribution of Social Security Numbers and Driver's License Numbers;
7. Security;
8. Notice;
9. Choice;
10. Access and Correctability;
11. Children; and
12. Compliance.

For additional information about the LexisNexis Data Privacy Policy contact the LexisNexis Privacy Manager at 1-800-831-2578 or by mailing:

Privacy Manager
LexisNexis
PO Box 933
Dayton, Ohio 45401

9. CHOICE - LexisNexis will allow certain individuals to opt-out of its non-public information databases containing sensitive information, under certain circumstances and conditions.

LexisNexis will consider a request for opt-out from its non-public information databases containing Social Security numbers in the following circumstances:

- The individual is a state, local or federal law enforcement officer or public official whose position exposes him or her to a threat of imminent harm;
- The individual is a victim of identity theft; or
- The individual is at risk of physical harm.

In order to have a request for opt-out considered, an individual must submit the following with the request, where applicable:

- If the individual is a law enforcement officer or public official, a letter from a supervisor must be submitted;
- If the individual is an identity theft victim, a copy of a police report documenting the individual's identity theft and an Identity Theft Affidavit must be submitted;
- If the individual is at risk of physical harm (other than as a law enforcement officer), a protective court order, a copy of a police report or similar documentation such as a letter from a social worker, a shelter administrator or a health care professional must be submitted.

In addition, LexisNexis will consider requests for opt-out for good cause. For all opt-out requests, LexisNexis retains the right to determine whether to grant or deny the request, the databases to which the request for removal will apply, and the duration of the removal period.

10. ACCESS & CORRECTABILITY – LexisNexis provides the public access to information about its products.

LexisNexis will upon request, inform individuals about the nature of the public records, non-public information, and publicly available information that LexisNexis makes available in its information products and services.

LexisNexis will

- Provide individuals with copies of non-public information about themselves contained in its information products and services for a nominal fee that is matched to the information provided by the individual;
- Take reasonable steps to verify an individual's identity prior to the release of any information to the individual;
- Direct individuals to the government and private entities which collect and maintain public records and publicly available information to correct any claimed inaccuracies found in that data; and
- Direct individuals to consumer reporting agencies where such agency is the source of the information about the individual and where the individual seeks to correct claimed inaccuracies found in that data.

For more information see the LexisNexis website

<https://web.lexis.com/ConsumerAccess/ConsumerAccess.asp>.

11. CHILDREN – LEXISNEXIS does not distribute information from non-public information files about people known to be under the age of 18.

Where an individual is identified in a record from a non-public information file as being under the age of 18, the information in that record about that individual will not be distributed by LexisNexis other than for activities such as the location of missing children or other law enforcement activities.

LexisNexis does not attempt to screen public records or publicly available information for references to individuals under the age of 18. Consequently, information about persons under the age of 18 may appear in these records.

12. COMPLIANCE – LEXISNEXIS will comply with its data privacy policy.

LexisNexis regularly monitors its business practices to ensure compliance with this Data Privacy Policy.