BIG DATA Handbook

5

Data Usage Agreements

Wolters Kluwer | BAKER BOTTS

Data Usage Agreements Introduction

The proliferation of the Internet of Things (IoT) has enabled widespread collection of data about nearly every aspect of the world around us. Once collected, this data can then be analyzed using Big Data and AI tools and techniques.[1] Together, IoT and Big Data provide a powerful combination of tools for identifying insights and drawing conclusions to optimize processes across all industries.[2] The usage of this data in this way is typically governed through, and in many cases limited by, data usage agreements (DUAs).[3]

DUAs are contractual agreements between a user, who generates data, and a data holder, broker, or analyst who collects, analyzes, or otherwise makes use of the user's data.[4] Potential users, or data subjects, include corporate clients and individual consumers. Analysts provide the technology that collects and analyzes users' data.[5] For purposes of this Handbook, all recommendations are assumed to be from the perspective of an analyst, and, except where otherwise noted, all users are assumed to be corporate users.

A DUA can include terms governing an analyst's rights to use and distribute data, data ownership, confidentiality requirements, security precautions, and other contractual terms negotiated between the parties. Additionally, such agreements must be mindful of federal and international data privacy laws and regulations, as well as state contract laws.

DUAs are the backbone of Big Data. Collecting and storing user data, which is often quite expensive, is not worthwhile without the ability to use that collected data to identify insights and commercial advantages. DUAs allocate those rights, responsibilities, and risks among the parties in a Big Data system, and can implicate concerns in connection with cybersecurity, intellectual property, and data privacy, among others. Accordingly, DUAs can touch upon and can be influenced by the topics discussed in the previous chapters of this Handbook.

---

1 Philip Kushmaro, *The IoT and Big Data: Making the Connection*, HUFFINGTON POST (Sept. 23, 2016, 3:49 PM), http://www.huffingtonpost.com/philip-kushmaro/the-iot-and-big-data-maki_b_12116608.html.

2 *Id*.

3 Doug Geisler, *Driving Data with Unintentional New Uses: Internet of Things*, AVNET, http://design.avnet.com/axiom/internet-things-creating-new-data-unintentional-new-uses (last visited July 28, 2017).

4 Peter Leonard, *Making the most of your data: Getting data analytics contracts right*, IAPP (Mar. 21, 2016), https://iapp.org/news/a/making-the-most-of-your-data-getting-data-analytics-contracts-right.

5 *Big Data Analytics Services*, HITACHI, https://www.hds.com/en-us/services/big-data-analytics-services.html (last visited July 28, 2017).

Best Practices for DUAs

DEFINING "DATA"

Before any further terms of a DUA are drafted, the scope of the term "data" should be clearly defined.[6] Data can be defined broadly or narrowly. Broad definitions of data, such as "any data generated by or derived from the user's activities and collected by the analyst," could result in the volume of data covered by the DUA changing significantly over time as more data may be collected. Narrow definitions of data, such as "data created by the user's activities in connection with locomotives and collected by analyst in the past five years," can more narrowly limit the types of data within the scope of the agreement.[7]

It is important that data be clearly defined in accordance with the expectations of the parties to a DUA. Depending on the needs of the parties, a broad or narrow definition may be appropriate. The parties should consider whether the agreement will cover data about, or generated by, the user or its customers, and whether "derived data" (i.e., new data generated through analysis of the original dataset), also sometimes referred to as "usage data," is within the scope of the agreement's definition of "data."[8]

In addition to defining the scope of covered data, the parties should agree on a format for data delivery. The agreement should specify a data format for delivery to the analyst that is useful and convenient. Additional considerations can include the frequency with which data will be updated, the mechanism for delivery, cybersecurity precautions, and the degree of support to be provided by the analyst.[9]

OWNERSHIP OF DATA

RAW DATA OWNERSHIP

DUAs should determine and clearly state which party will own any data contemplated within the scope of the agreement.[10] Typically, the user, or data subject, will retain ownership of the data and license it to the analyst; however, a DUA can alternatively provide for data ownership to transfer from the user to the analyst.[11] The DUA should also specify the ownership of derived data or other results of data analysis—often the subject of great

---

[6] David W. Tollen, *The Big Data Licensing Issue-Spotter*, TECHCONTRACTS.COM (Dec. 8, 2015), https://techcontracts.com/2015/12/08/the-big-data-licensing-issue-spotter/#_ftn4.

[7] *See id.*

[8] *Id.*

[9] *See id.*

[10] *Id.*; *see Cutting Edge Issues in IP Ownership: Big Data and New Technologies*, ASSOCIATION OF CORPORATE COUNSEL 1, 14-15 (June 1, 2016), https://www.acc.com/chapters/wash/upload/BakerHostetler-Cutting-edge-issues-in-IP-ownership.pdf [hereinafter *IP Ownership*].

[11] Tollen, *supra* note 6; *see* Leslie T. Thornton & Edward R. McNicholas, *Governing Information with Vendors–Contracting with Service Providers*, 5 Successful Partnering Between Inside and Outside Counsel § 82.17 (2015).

debate, and fierce negotiation, in connection with DUAs.[12] The commercial realities and details of any given agreement will determine which approach is best.

When ownership is retained by the user, a preservation clause can be included to that effect. A preservation clause might state, for example, that: "The Licensed Data remains User's sole and exclusive property, and Analyst receives no right, title, or interest in or to the Licensed Data, except to the limited extent set forth in the Data License."[13]

When ownership is transferred from the user to the analyst, an assignment clause can be included to that effect. For example, an assignment clause might state that: "User hereby assigns all its right, title, and interest in and to the Transferred Data to Analyst."[14]

DERIVED DATA OWNERSHIP

Licensing of data often results in the generation of new data. "Derived data," or "usage data" generally refers to data generated through analyzing and processing the original dataset, and through monitoring or observing the use of the system. It may also include derivative works, such as modified versions of the original dataset to which additional data has been added or from which data has been removed.[15]

The scope and ownership of derived data should be clearly defined in a DUA. Derived data may be defined broadly to include derivative works, or it may be defined more narrowly, to separate other derived data from derivative works. Both analysts and users may want ownership of derived data. Users may argue that because derived data results from the original dataset, which the user owns, and without which the derived data could not have been generated, the user should rightly own the derived data. Analysts may argue that the derived data results from the analyst's transformation of the dataset—which is not possible without the analyst's processing engine—so it should be owned by the analyst.[16] Again, the outcome of each such negotiation will be determined by the commercial realities and respective bargaining positions of the parties.

In determining ownership of derived data, the user may want to know whether original data can be retrieved from the derived dataset. If so, users may be unlikely to agree to terms transferring ownership of the derived data to the analyst. The user may also consider whether the derived dataset is, or can be, anonymized, and if so may be more likely to cede ownership to the analyst.[17]

LICENSING BACK

One way to facilitate agreement over data ownership is to include a license back provision in the DUA. Under a license back, whichever party grants ownership of the data under the agreement receives a license to use the data. Licensing back may allow the party that does not own the derived data to nevertheless use and exploit the results of the analyst's work. Additionally, when the agreement calls for ownership of the raw data to pass to the analyst, the user may want a license back to maintain access to the data. When the user retains ownership of the raw data,

---

[12] Tollen, *supra* note 6.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *See id.*
[17] *See id.*

the analyst typically does not need a license back because the direct license between the user and the analyst will usually suffice. If a license back is used, it should clearly set forth what data and usage rights fall within its scope, and may include usage restrictions and distribution restrictions, as discussed below.

OWNERSHIP OF INTELLECTUAL PROPERTY

COPYRIGHT

Big Data presents unique intellectual property questions. While the raw data itself in many instances may not be subject to any intellectual property protections,[18] the original arrangement or compilation of the raw data may be protected under copyright law.[19] According to the U.S. Copyright Office, "[a]n application to register a database typically covers the selection, coordination and/or arrangement of data, information or files, but does not cover the data, information or files unless they are specifically claimed in the application."[20] The EU approach differs slightly, and provides copyright protection of a database if there has "been substantial investment in obtaining, verifying, or presenting the contents of the database."[21]

Under U.S. copyright law, a copyright owner has the exclusive right to create derivative works based on their copyrighted work.[22] A copyright owner "may claim copyright in a work that recasts, transforms, or adapts a [copyrighted] work."[23] An exception to derivative works exists under the fair use doctrine.[24] Under the fair use doctrine, courts analyze four factors to determine whether a derivative work constitutes a fair use, such that there is no copyright infringement.[25] The factors include: (1) "the purpose and character of the use," (2) "the nature of the copyrighted work," (3) "the amount and substantiality of the portion used in relation to the copyrighted work as a whole," and (4) "the effect of the use upon the potential market for or value of the copyrighted work."[26] Under the first factor, "the purpose and character of the use," courts will look to whether the use is transformative, "altering the original with new expression, meaning, or message."[27]

---

[18] *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 344 (1991) ("Facts are not copyrightable."); *see IP Ownership*, *supra* note 10, at 17.

[19] *Feist Publ'ns, Inc.*, 499 U.S. at 348 ("[The compilation author's] choices as to selection and arrangement, as long as they are made independently by the compiler and entail a minimal degree of creativity, are sufficiently original that Congress may protect such compilations through the copyright laws."); *Gemel Precision Tool, Co. v. Pharma Tool Corp.*, 1995 WL 71243, at *4 (E.D. Pa. Feb. 13, 1995) ("While it is true that factual information generally accessible to the public is not protected by copyright law, the compilation of those facts may be copyrightable."); *see IP Ownership*, *supra* note 10, at 17.

[20] *U.S. COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 1002.6* (3d ed. 2014) [hereinafter COMPENDIUM]; *see IP Ownership*, *supra* note 10, at 18.

[21] EU Directive 96/9/EC on the Legal Protection of Databases; *see IP Ownership*, *supra* note 10, at 19.

[22] COMPENDIUM, *supra* note 20 § 507.2; *see IP Ownership*, *supra* note 10, at 23.

[23] COMPENDIUM, *supra* note 20 § 507.2.

[24] Copyright Act of 1976, 17 U.S.C. § 107.

[25] *Id.*; *see* More Information on Fair Use, COPYRIGHT.GOV, https://www.copyright.gov/fair-use/more-info.html (last visited July 28, 2017).

[26] 17 U.S.C. § 107.

[27] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 569 (1994).

A key question, therefore, is whether Big Data analysis transforms a dataset.[28] On the one hand, analysts may argue that their analysis provides the original dataset with new meaning and transforms the dataset.[29] On the other hand, users may argue that the change is not so great that it meaningfully transforms the copyrighted database.[30] To avoid these types of copyright conflicts over the original dataset and the derived data, IP ownership should be clearly allocated in a DUA.[31]

Additionally, because ownership of the original dataset will often remain with the user, analysts should receive licenses to the dataset to prevent copyright infringement litigation over their agreed-upon work.[32]

TRADE SECRET

Data may also constitute or include a user's protected trade secrets.[33] Users may require reasonable internal and external procedures to protect their trade secrets.[34] Accordingly, users may seek to impose restrictions, including confidentiality requirements (as further discussed below), data security requirements, and limitations on the number of people privy to trade secret information.[35] The parties to the DUA should agree on the appropriate terms to protect and maintain trade secret status of any trade secret information.[36] Breach of these terms by the analyst can threaten the user's trade secrets as well as the analyst's commercial relationship with the user.[37]

LICENSE SCOPE

A DUA should define the scope of the analyst's license to the user's data by delineating data usage rights, data use restrictions, and data distribution restrictions.[38] Analysts will typically seek expansive licenses to users' data, including broad usage rights, minimal use restrictions, and broad distribution rights, while users, or data subjects, may wish to only grant narrow licenses with specific usage rights, strict use restrictions, and limited distribution rights.[39]

DUAs AND USAGE RIGHTS

Data usage rights define the breadth of the analyst's rights to use the user's dataset. It is typically important, from the perspective of a data analyst, to secure broad usage rights to have flexibility in the use of the data because the value and monetization of Big Data datasets is typically driven in part by the ways in which the data can be used. Seeking broad usage rights, analysts may sometimes be granted data access without restriction or limitation, for a

---

[28] *See IP Ownership*, *supra* note 10.
[29] *See id.*
[30] *See id.*
[31] *See* Tollen, *supra* note 6.
[32] *See id.*
[33] *See IP Ownership*, *supra* note 10, at 23; Tollen, *supra* note 6.
[34] *See* Tollen, *supra* note 6.
[35] *Id.*
[36] *See id.*
[37] *See id.*
[38] *Id.*
[39] *See id.*

fee. An agreement resulting from such an arrangement could recite, for example: "User hereby grants Analyst a non-exclusive right to reproduce and modify the data."[40]

Users may attempt to constrain usage rights through a narrow license, using more restrictive language, for example: "User hereby grants Analyst a non-exclusive right to reproduce the data and use it as set forth in the Data Use Section and to modify the data solely as set forth in the Data Modification section."[41] Of course, such a DUA would also need to define the allowable usage and modification of the data.[42]

Alternatively, usage rights can be crafted broadly, and usage restrictions can be imposed on this right. This approach provides the analyst unfettered access to the data, but constrains the analyst's usage via restrictions, as discussed below.[43]

DUAs AND USAGE RESTRICTIONS

Usage restrictions enable the user to limit the scope of a data license.[44] Examples of potential use restrictions include, among others, customer restrictions, field of use restrictions, consumer restrictions, anonymity requirements, sub-licensing restrictions, exclusivity restrictions, and discovery restrictions.[45] A wide variety of creative usage restrictions may be crafted.

Customer restrictions limit the third parties for whom the analyst may provide services based on analysis of the user's dataset.[46] The user may want its data used solely for it, and could request a restriction such as: "User's data shall be used by Analyst only to provide services to User." Similar but less stringent restrictions could be employed, for example, prohibiting the analyst from providing services to direct competitors of a customer. The power of Big Data, however, lies in the aggregation of data and the use of combined datasets to serve many different functions. The analyst is therefore typically incentivized to bargain for less restrictive usage rights, and to try to leverage the data available to it.

Field of use restrictions may limit the analyst's ability to do anything more than provide services to the user. These restrictions may limit the analyst's ability to use the user's dataset to identify, market, advertise to, or contact the user's consumers. Field of use restrictions may also be used to limit the territory where the data may be stored, processed, or accessed, or may provide limitations on the devices that may store, process, or access the data.[47] The user may want to impose narrow field of use restrictions. The analyst might not have a strong preference on field of use restrictions, so in some circumstances, the analyst may be able to use field of use restrictions as a bargaining chip to obtain concessions in other areas that are more critical to an analyst's business.

If the data was collected from the user's consumers, then consumer restrictions may limit the analyst so that promises made to the user's consumers when the data was collected, are kept. The user must insist that the

---

[40] *Id.*
[41] *Id.*
[42] *See id.*
[43] *See* Tollen, *supra* note 6.
[44] *See id.*; Thornton & McNicholas, *supra* note 11.
[45] *See* Tollen, *supra* note 6.
[46] *See id.*
[47] *Id.*

analyst not use its data in any manner inconsistent with the user's agreement with its consumers. Consumer restrictions are crucial to the user because such restrictions can help the parties avoid or at least minimize the risk of potential lawsuits from consumers.[48] The analyst may need to acquiesce to these restrictions, but it can still use them to bargain for other concessions from the user.

Anonymity requirements may obligate the analyst to analyze only anonymized data and may set restrictions on the analyst's usage rights for the anonymized data. As further discussed in the privacy chapter, data can be anonymized by removing identifying information, such as names and other personal information of consumers, from the dataset. The analyst, in accordance with an agreement may be obligated to anonymize the data, or the user may provide the analyst with an anonymized dataset.[49] In either case, and depending on the context of the agreement and the source of the data (e.g., was the data collected from human data subjects or some industrial IoT data gathering), a user may seek to impose restrictions on the analyst's ability to extract or discern identifying information from the anonymized dataset.[50]

Sub-licensing must be expressly authorized or forbidden. When sub-licensing is authorized, a user may generally seek to delineate the permissible purposes of any sub-license and may seek to restrict the list of authorized sub-licensees. Additionally, the user may want any sub-licensee to be bound by the DUA, including any usage restrictions provided in the DUA. Liability for the sub-licensee's conduct should also be addressed in any DUA that provides for sub-licensing. While neither the user nor the analyst will be incentivized to bear the risk of liability for a sub-licensee's conduct, the user and the analyst should seek to specify in the agreement the liability allocation as between the parties. An analyst may have a stronger argument against bearing this risk if the DUA provides for user approval of any sub-licensee. The analyst can also try to avoid any sub-licensing issues by requiring that the user contract directly with any third parties.[51]

Exclusivity restrictions may govern who may exploit the data under the DUA. DUAs may be non-exclusive agreements, providing that the user and third parties can also use the data. Under an exclusive agreement, however, the analyst may be granted the sole right to use the data, such that the user and any third parties will not be able to use the data without the analyst's consent. These issues should be clearly resolved in the DUA by including exclusivity or non-exclusivity clauses.[52] Exclusivity clauses can be tailored to allow data access to certain parties, but not others (for example, competitors, other companies operating in particular industries, etc.).

Discovery restrictions can be included to create procedures for situations in which the data that is the subject of a DUA becomes the subject of discovery in a litigation. If the data is solely in the analyst's possession, then the analyst may be subpoenaed by opposing parties or third parties in litigation. Therefore, the user and analyst should agree on terms governing discovery considerations. By employing these procedures, if the user has access to the data and that data is sought in discovery, the user can respond to discovery requests more efficiently without requiring involvement of the analyst. In the context of discovery restrictions, parties should also consider

---

[48] *Id.*
[49] *Id.*
[50] *See id.*
[51] *Id.*
[52] *See id.*

retention and deletion. To avoid the risk of sanctions for spoliation,[53] the DUA may also provide that either the user maintain a copy of an unaltered dataset or that the analyst preserve a copy of an unaltered dataset before any data is modified or deleted.[54]

DUAS AND DISTRIBUTION RESTRICTIONS

A license may also include distribution restrictions. Distribution restrictions determine whether the analyst may redistribute the raw data or an anonymized version of the data set.[55] Because distribution of the raw data can extinguish trade secret protection of the data, a user in some circumstances may want to strictly limit any such redistribution.[56] Additionally, redistribution could result in liability for a breach of a user's agreement with its consumers or data subjects, or consumers may be displeased to learn that a user is allowing redistribution of the consumers' data.[57] As a result, the user may be reluctant to allow redistribution of the raw data. At a minimum, the user will often want to place limits on the parties to whom data may be distributed and might require that any redistribution comply with the data usage restrictions.[58]

COMPLIANCE CONDITIONS

The DUA may condition usage rights on certain performance requirements.[59] The user may seek to expressly condition the license on compliance by the analyst with other provisions of the DUA, such as the data usage restrictions, data distribution restrictions, anonymization requirements, confidentiality requirements, and security requirements.[60] A breach of the compliance conditions would therefore invalidate the license and cause the analyst to both breach the contract and become an infringer of any IP rights covered by the license.[61] Even if the user fails to include an express compliance condition in the DUA, the DUA may include an inherent compliance condition, as a material breach of the DUA may result in contract termination.[62]

CONFIDENTIALITY

Both the user and the analyst will want to ensure that data is kept confidential.[63] The user will generally want the analyst to keep the raw data confidential and the analyst will generally want the user to keep the derived data confidential.[64] To ensure confidentiality, the DUA should include an express confidentiality clause, such as: "Analyst and User will not disclose the data or derived data or any part of it to any third party except as specifically

---

[53] *See id.*
[54] *See id.*; Thornton & McNicholas, *supra* note 11.
[55] Tollen, *supra* note 6.
[56] *Id.*
[57] *Id.*
[58] *Id*.
[59] *Id*.
[60] *See id.*
[61] *Id.*
[62] *See id.*
[63] *See id.*
[64] *Id.*; *see* Thornton & McNicholas, *supra* note 11.

authorized by this Agreement."[65] As included in the above example, the confidentiality clause must include an exception clause that exempts specific authorizations in the DUA from confidentiality requirements.[66] The exception clause keeps the confidentiality requirement from frustrating other provisions of the DUA, such as those authorizing distribution to third parties and sub-licensing.[67]

The parties should also specify an appropriate term for the confidentiality clause. For example, confidentiality requirements could last for the term of the DUA, or continue beyond it. The particular facts of any given Big Data transaction, and the data that is the subject of the agreement, will be factors that determine the length of the term. Confidentiality may also raise concerns related to trade secrets, and if a DUA covers trade secret information, a confidentiality clause should not expire as long as the data is held as a trade secret.[68]

SECURITY

Data security clauses govern the precautions that each party will take in protecting the data from unauthorized exposure or disclosure.[69] Potential precautions include technical steps such as data encryption, passwords, and data breach detection software, and physical steps, such as locking the doors to server rooms, as more fully explored in the cybersecurity chapter.[70] The DUA should clearly state which party is responsible for taking which security measures, and which party is responsible in the event of a data breach.[71] The analyst in a typical agreement will likely be required to take data security measures.[72]

The analyst may also be required to monitor for potential data breaches and provide notice to the user in the event of a breach.[73] The DUA should clearly state the analyst's responsibilities in the event of a data breach.[74] Considerations include the level of monitoring that the analyst is required to conduct, the type of notice that the analyst is required to provide the user, and the level of cooperation the analyst is required to provide to the user and law enforcement in the event of a breach.[75]

WARRANTIES AND INDEMNITIES

The analyst may also wish to seek warranties and indemnities from the user.[76] The user may want to disclaim any warranties related to their data, and to provide the data "as is."[77] Such a disclaimer clause could recite: "Data is provided 'as is,' without warranty of any kind, either expressed or implied, including without limitation any

---

[65] Tollen, *supra* note 6.
[66] *Id.*; *see* Thornton & McNicholas, *supra* note 11.
[67] *See* Tollen, *supra* note 6.
[68] *See id.*
[69] Tollen, *supra* note 6; *see* Thornton & McNicholas, *supra* note 11.
[70] Tollen, *supra* note 6.
[71] *See id.*.
[72] *See id.*
[73] *Id.*; *see* Thornton & McNicholas, *supra* note 11.
[74] Tollen, *supra* note 6.
[75] *Id.*
[76] *Id.*
[77] *Id.*

warranties that the data is fit for a particular use."[78] The analyst may, however, refuse such a broad disclaimer and insist on some warranties from the user, such as IP warranties or warranties that the user has taken reasonable measures to ensure data accuracy and/or integrity.[79]

In addition to warranties, the parties can craft indemnities to shift liability between the parties in the event of a lawsuit.[80] Particular indemnities will depend on the terms of the contract; however, a typical DUA will include some form of data breach indemnities.[81] Data breach indemnities may result in the user indemnifying the analyst, the analyst indemnifying the user, or a mutual indemnity in which both parties agree to indemnify each other under certain circumstances.[82] Indemnity clauses should be drafted so that they are consistent with other contractual terms.[83]

LIQUIDATED DAMAGES

Damages arising from a DUA breach can be difficult to quantify.[84] Accordingly, a DUA may include a liquidated damages clause in the event of a breach.[85] A liquidated damages clause provides the user and the analyst with more certainty and allows the parties to better allocate their risk and resources in connection with the transaction. An example of a liquidated damages clause may include language along the lines of: "Whereas the parties agree that quantifying damages arising from a breach of this agreement is inherently difficult, in the event that User breaches this agreement, User shall pay Analyst $[x]; and in the event that Analyst breaches this agreement, Analyst shall pay User $[y]."

TERMINATION

One of the final considerations for the parties to a DUA is the question of what happens with the data upon termination of the DUA. Considerations include returning raw data and derived data, destroying raw data and derived data, and transition services.[86] In some agreements, raw data is returned to the user upon termination of the DUA.[87] The DUA should define the timing for the return of raw data, and should specify the format in which data should be returned.[88] Additionally, if the derived data is owned by the user, the analyst may be required to

---

[78] *See id.*
[79] *See id.*
[80] *See id.*
[81] *See id.*
[82] *Id.*
[83] For example, the indemnification provision must be consistent with the security requirements. If, on the one hand, the DUA states that the analyst is responsible for security measures and the analyst fails to meet those measures, resulting in a data breach, the indemnification provision may dictate that the analyst must indemnify the user. If, on the other hand, the analyst meets those measures, but a data breach still occurs, the indemnification provision may dictate that the user agrees to indemnify the analyst.
[84] *See* Tollen, *supra* note 6.
[85] *Id.*
[86] *See id.*
[87] *Id.*
[88] *Id.*

return the derived data to the user.[89] Similar to the raw data, specific terms as to the return of derived data should be explicitly included in the DUA.[90]

The DUA may require that the analyst destroy data upon termination.[91] An example of such a destruction clause is: "Analyst will destroy any and all copies of the User's data in its possession or control, exercising reasonable efforts to ensure that no element of the data may be restored by any means."[92] Similar to the return of data, a destruction clause should specify the time for performance.[93]

Finally, a DUA should include transition terms if a user contemplates transferring its data to a new analyst.[94] The user may not be able to conveniently manage or store its data until it identifies a new analyst.[95] Such a user may seek to include transition terms to ensure safe management and storage of the data during such a transition.[96] For continuity, the DUA can include transition terms requiring the analyst to continue to store the data for the user while granting the user continuing access.[97] The terms can also require storage for a set period of time.[98] Analysts may also wish to require a fee associated with these transitional services.[99]

LEGAL COMPLIANCE

A DUA should also specify that the parties are required to comply with all applicable laws and regulations.[100] For example, such an agreement may include a provision requiring compliance with applicable laws and regulations related to data privacy, such as those more fully explored in the privacy chapter of this Handbook.[101] Such a provision may help to ensure compliance with applicable state and federal data privacy laws. Ultimately, a DUA will be subject to state contract law in the event of a dispute between the user and the analyst.[102]

When U.S. law governs the DUA, applicable federal laws may include the Health Information Portability and Accountability Act ("HIPAA"), [103] the Fair Credit Reporting Act ("FCRA"), and the Gramm-Leach-Bliley Act ("GLBA").[104] Additional federal regulations from the FTC may also be applicable.[105] States may also have individual

---

[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *See id.*
[93] *See id.*
[94] *See id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *See id.*
[101] *Id*.
[102] *See* Tollen, *supra* note 6.
[103] *See* Kevin Coy & Neil W. Hoffman, *Big Data Analytics under HIPAA*, ARNALL GOLDEN GREGORY LLP (March 17, 2016), http://www.agg.com/Big-Data-Analytics-Under-HIPAA-03-17-2016/.
[104] *See* Tollen, *supra* note 6; Jacqueline Klosek, *Regulation of Big Data in the United States*, TAYLORWESSING (July 2014), https://www.taylorwessing.com/globaldatahub/article_big_data_us_regs.html.

data privacy laws, such as the California Online Privacy Protection Act ("CalOPPA"), and data regulations, such as the Massachusetts Data Security regulations.[106] When EU law governs a DUA, the EU General Data Protection Regulation ("GDPR") will likely apply to a DUA.[107]

The bottom line: DUAs can invoke a quagmire of laws and regulations from many different jurisdictions, and as a result, require counsel across a broad spectrum of legal expertise to ensure compliance.

OTHER CONSIDERATIONS

The universe of potential terms for a DUA is broad and includes many other provisions that are beyond the scope of this Handbook, including provisions common to general corporate contracts and technology agreements, such as definitions of termination, third party assignment provisions, payment terms, and further liability clauses.[108]

---

[105] *See* John K. Higgins, *FTC Issues Regulatory Warning on Big Data Use*, E-Commerce Times (Jan. 20, 2016), http://www.ecommercetimes.com/story/83004.html; Klosek, *supra* note 104.

[106] *See* Tollen, *supra* note 6; Klosek, *supra* note 104.

[107] Tollen, *supra* note 6.

[108] *Id.*