Deloitte.

DME Tax Genie 2.0 - Rules of the Road

The Deloitte AI Institute together with the Deloitte Middle East Tax & Legal practice has developed Tax Genie 2.0 to provide a safe and secure environment to use Generative AI. Think of it as a ChatGPT specifically for Deloitte, where you can do things such as create PowerPoints, emails, proof-read and check code.

In line with the Deloitte Shared Values, you are responsible for following these Rules of the Road when accessing Tax Genie 2.0:

You can input/upload:

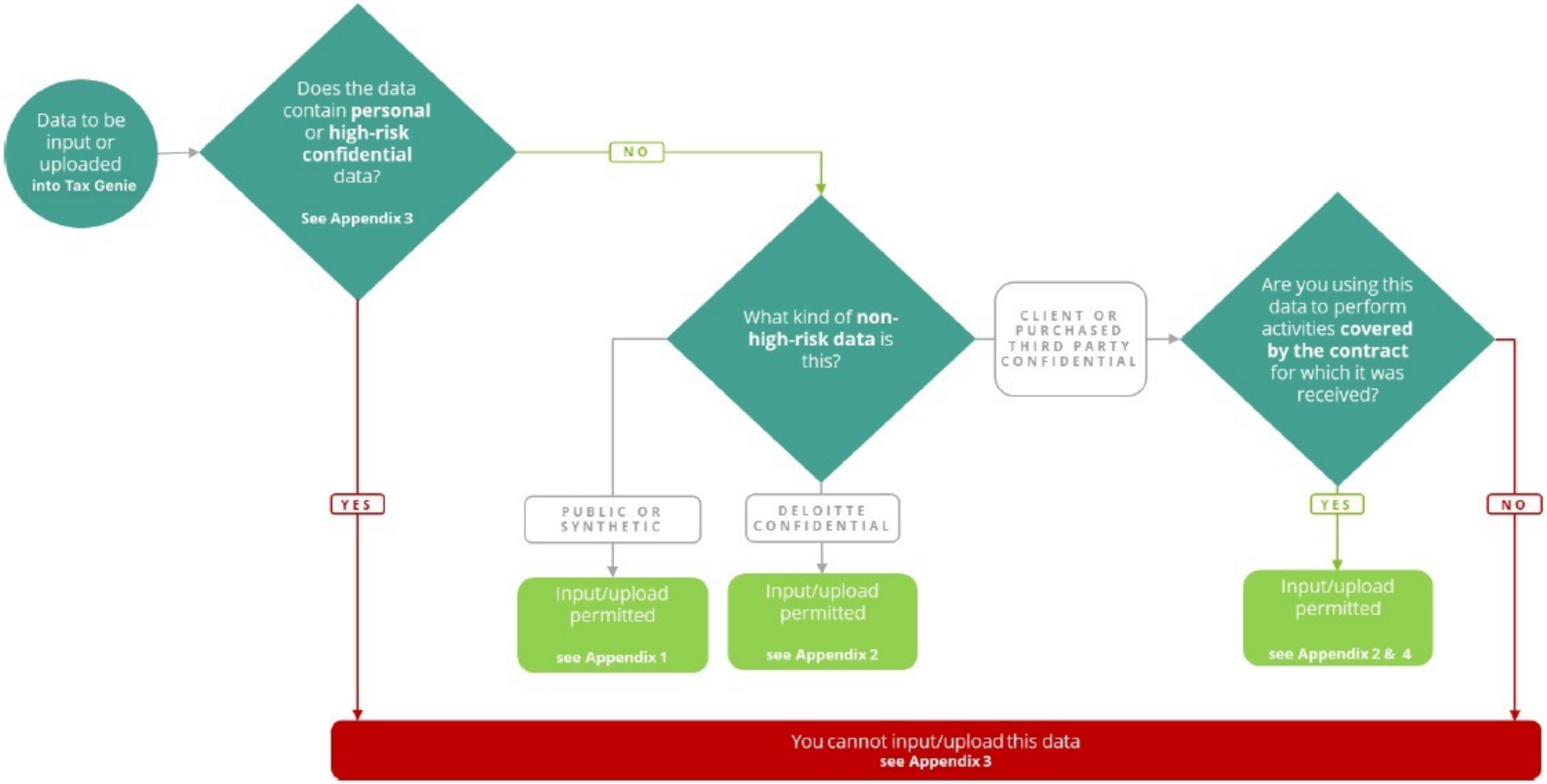
- Client and purchased third party Confidential data being used to perform the contractual purpose(s) under which it was received and for which no regulatory, sector specific, contractual or other restrictions apply (see Appendix 2 and Appendix 4)
- Deloitte data classified as Public or Confidential originating from your member firm/geo or where you otherwise have approval from the data owner to reuse content (see Appendix 2)
- Public or Synthetic data (which is free to use in the public domain other than Personal Data, or for which a license has been obtained – see Appendix 1)

Do not input/upload:

- Personal data (see Appendix 3)
- High Risk Confidential data (see Appendix 3)
- Data classified as Confidential (including that from clients and other third parties) being reused for a secondary purpose that is not expressly allowed by the contract/license/terms under which it was received and/or where the contract/license/terms explicitly does not permit the use of Generative AI or cloud environments. If in doubt, consult with your local QRM team - see Appendix 2 for more details.
- Client confidential data where the client has specifically given instructions restricting the use of an AI tool or ONLY permits the use of an AI tool developed by the client.
- Client confidential data whereby the client has classified such data as ‘Internal Only’, ‘Confidential’ ‘Restricted’ or data pertaining to KSA government entities: ‘Confidential’, ‘Secret’ and ‘Top Secret’.

Deloitte.

Use the following flow to help you work out what data you can and can't use within Tax Genie 2.0:


Data to be input or uploaded into Tax Genie
Does the data contain personal or high-risk confidential data?
See Appendix 3
NO
YES
What kind of non-high-risk data is this?
PUBLIC OR SYNTHETIC
DELOITTE CONFIDENTIAL
CLIENT OR PURCHASED THIRD PARTY CONFIDENTIAL
Are you using this data to perform activities covered by the contract for which it was received?
YES
NO
Input/upload permitted
see Appendix 1
Input/upload permitted
see Appendix 2
Input/upload permitted
see Appendix 2 & 4
You cannot input/upload this data
see Appendix 3

Please take note when using Tax Genie 2.0:

- Use one chat for each client, you can have several chats running simultaneously. This will ensure confidential data from one client is not mixed with data from another, and ensure compliance with the RotR.
- Before you upload data to Tax Genie 2.0, make sure the classification label aligns with the actual content and the allowed data classifications listed above.

When reviewing the output from Tax Genie 2.0, you must:

- remember that Tax Genie 2.0 is a tool, and may not be 100% accurate and/or complete;
- check the work yourself to make sure the Tax Genie 2.0 output is correct before using it in any way (e.g. copying and pasting into your work);
- put the output through your existing review and quality assurance process, including through the Engagement Manager, with extra care if the output is going to a client/third party;
- remember that Tax Genie 2.0 is an information tool, and do not treat or consider any output as a confirmed or compliant Deloitte view/position (including answers to specific questions that have been input);
- Tax Genie 2.0 is not a replacement for Subject Matter Experts, and you must consult with them as needed e.g. your local QRM, QRS, Legal, Data Privacy teams, etc.;
- Ensure brand and legal disclaimers are included in any outputs (where required/applicable) – in case of doubt contact your local QRM/QRS/Legal teams;
- note that the underlying data source used is from the internet as at April 2023 (see the limitations that Microsoft note here).

Output classification: Tax Genie 2.0 generated output does not inherit permissions or data classification labels from the input data. If you use the output, make sure the document where it is used is of the same classification or higher.

Permitted use: must be for business purposes in line with these Rules of the Road and our ethics and values, considering our Trustworthy & Ethical Tech principles as well as any other applicable local rules/standards/policies/guidelines.

Prohibited use: Tax Genie 2.0 must not be used beyond the scope and purposes set out in these Rules of the Road, and you must not use Tax Genie 2.0 output in place of subject matter expertise you are expected to provide within your role. This includes using any generated output in place of your own knowledge and judgement, for example, as part of any professional training, in house or professional examinations/assessments, interviewing or where trust is being placed on your own knowledge and expertise.

Access: as with any other Deloitte system or application you must not share your access and/or provide access via your Deloitte account to anyone else (see your local confidentiality, privacy and security policy for further information).

Residency: Your Tax Genie 2.0 platform will be specific to your geography, and you are expected to comply with the laws and regulations for your Geography, including data protection legislation, and any relevant regulations on cross border transfer of confidential information. If in doubt, consult your local QRM team.

Scope: these Rules of the Road apply to the Tax Genie 2.0 environment only (inclusive of inputs/prompts used and onward use of outputs) and are to be followed in addition to general acceptable use of Deloitte systems as per your local security policy and adherence with the firm's ethical and diversity standards as per the NSE Code of Conduct. The availability and guidance for other Generative AI environments under enterprise agreements will be published as they become available on the Global Generative AI site. Until then the interim NSE guidance continues to apply for the usage of any other Generative AI tools.

Issue/error reporting: if you observe any unusual or unexpected output (e.g. content that doesn't make sense) you must make a note of the output and the input that generated it and report this via email to the Tax Genie 2.0 team and by raising a ticket via Service Now to your local IRT Team without undue delay.

Accidental input/output reporting: if you accidentally input any prohibited data (as defined above) or observe output that could be seen as such, then you must report this as a privacy/confidentiality incident through your geography's asset and data loss process / IT Helpdesk.

If you have any questions, take a look at the Tax Genie 2.0 FAQs and if you have any other questions or if you have a technical query, please contact your local IT support team. If you have any QRM related questions, please contact your local QRM team.

Appendices – Introduction to Data Guardrails

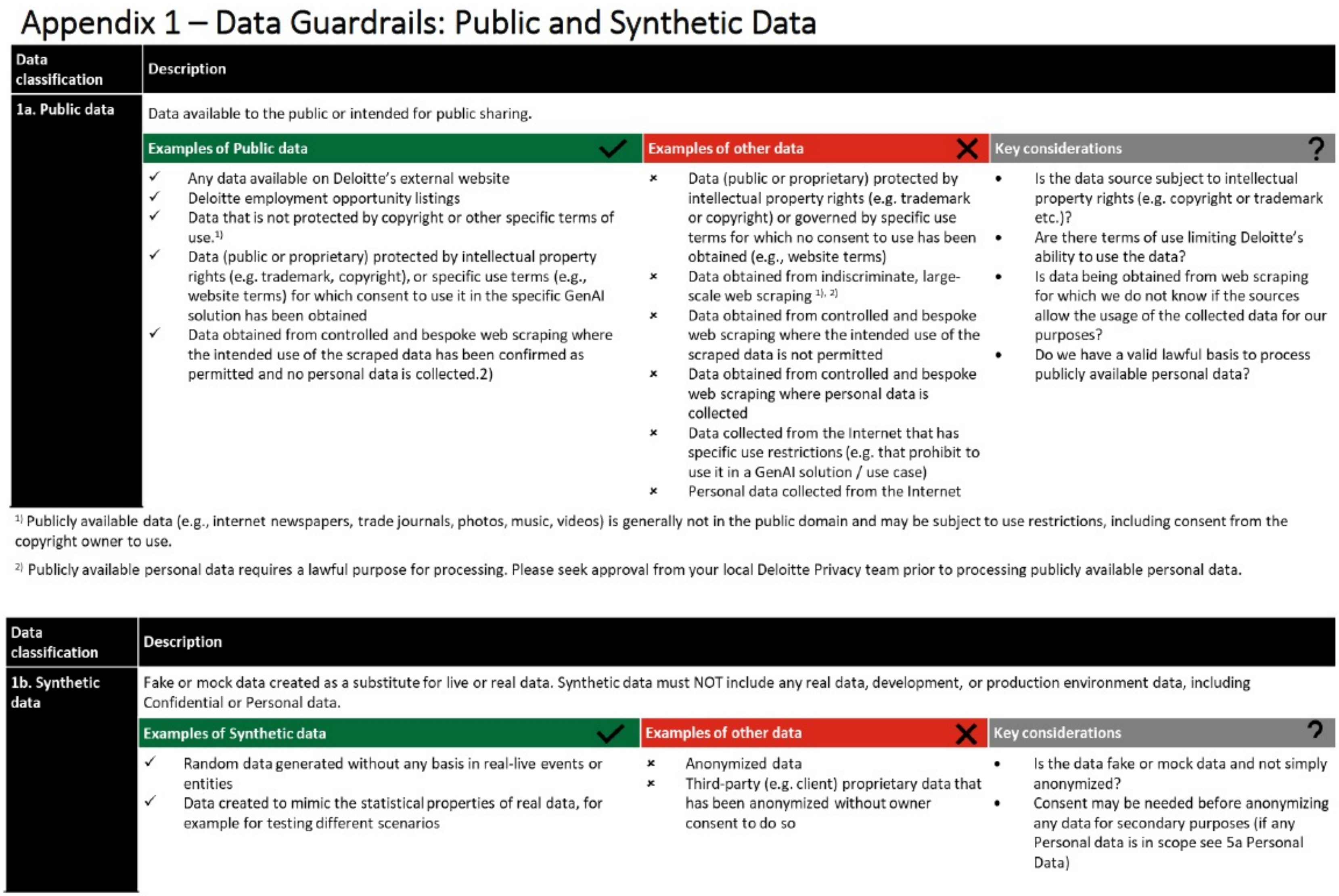
These appendices will give you examples of the data that is currently permitted and not permitted to be put into Tax Genie 2.0. We will update these in the future as our maturity as a firm continues to grow.

When we refer to 'data' we may initially think of text and documents, but data takes many forms and these Rules of the Road apply to data in all forms. Data is a wide term referring to all raw, uncategorised, processed and categorised facts.

Data can be structured or unstructured:

- Structured data is data that has been organised into a formatted repository like a database, so that its contents can be easily searched, processed or analysed.
- Unstructured data is data which does not fit in a traditional row-column database. Examples include Microsoft Word, or PowerPoint, emails, PDFs, audio/video, photos or webpages. While these sorts of files may have an internal structure, they are still considered "unstructured".

The following data guardrails should be read with all forms of data in mind.



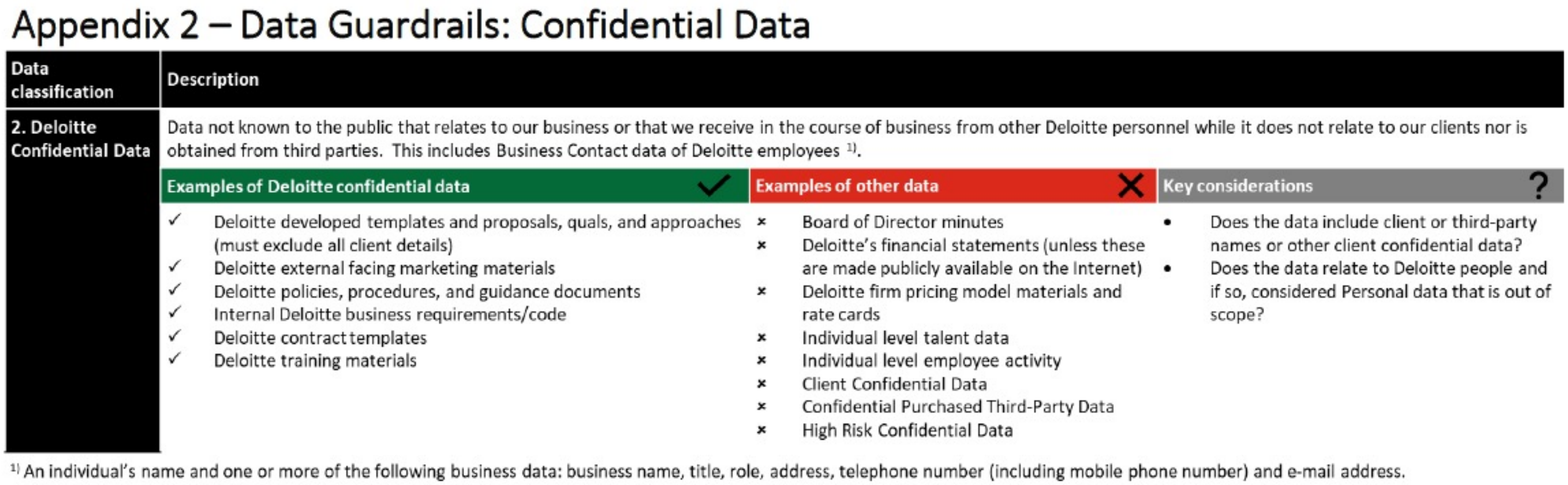
Appendix 1 – Data Guardrails: Public and Synthetic Data

Data classification	Description		
1a. Public data	Data available to the public or intended for public sharing.		
	Examples of Public data ✓	Examples of other data ✗	Key considerations ?
	✓ Any data available on Deloitte's external website ✓ Deloitte employment opportunity listings ✓ Data that is not protected by copyright or other specific terms of use.[1] ✓ Data (public or proprietary) protected by intellectual property rights (e.g. trademark, copyright), or specific use terms (e.g., website terms) for which consent to use it in the specific GenAI solution has been obtained ✓ Data obtained from controlled and bespoke web scraping where the intended use of the scraped data has been confirmed as permitted and no personal data is collected.2)	× Data (public or proprietary) protected by intellectual property rights (e.g. trademark or copyright) or governed by specific use terms for which no consent to use has been obtained (e.g., website terms) × Data obtained from indiscriminate, large-scale web scraping [1], [2] × Data obtained from controlled and bespoke web scraping where the intended use of the scraped data is not permitted × Data obtained from controlled and bespoke web scraping where personal data is collected × Data collected from the Internet that has specific use restrictions (e.g. that prohibit to use it in a GenAI solution / use case) × Personal data collected from the Internet	• Is the data source subject to intellectual property rights (e.g. copyright or trademark etc.)? • Are there terms of use limiting Deloitte's ability to use the data? • Is data being obtained from web scraping for which we do not know if the sources allow the usage of the collected data for our purposes? • Do we have a valid lawful basis to process publicly available personal data?

[1] Publicly available data (e.g., internet newspapers, trade journals, photos, music, videos) is generally not in the public domain and may be subject to use restrictions, including consent from the copyright owner to use.

[2] Publicly available personal data requires a lawful purpose for processing. Please seek approval from your local Deloitte Privacy team prior to processing publicly available personal data.

Data classification	Description		
1b. Synthetic data	Fake or mock data created as a substitute for live or real data. Synthetic data must NOT include any real data, development, or production environment data, including Confidential or Personal data.		
	Examples of Synthetic data ✓	Examples of other data ✗	Key considerations ?
	✓ Random data generated without any basis in real-live events or entities ✓ Data created to mimic the statistical properties of real data, for example for testing different scenarios	× Anonymized data × Third-party (e.g. client) proprietary data that has been anonymized without owner consent to do so	• Is the data fake or mock data and not simply anonymized? • Consent may be needed before anonymizing any data for secondary purposes (if any Personal data is in scope see 5a Personal Data)

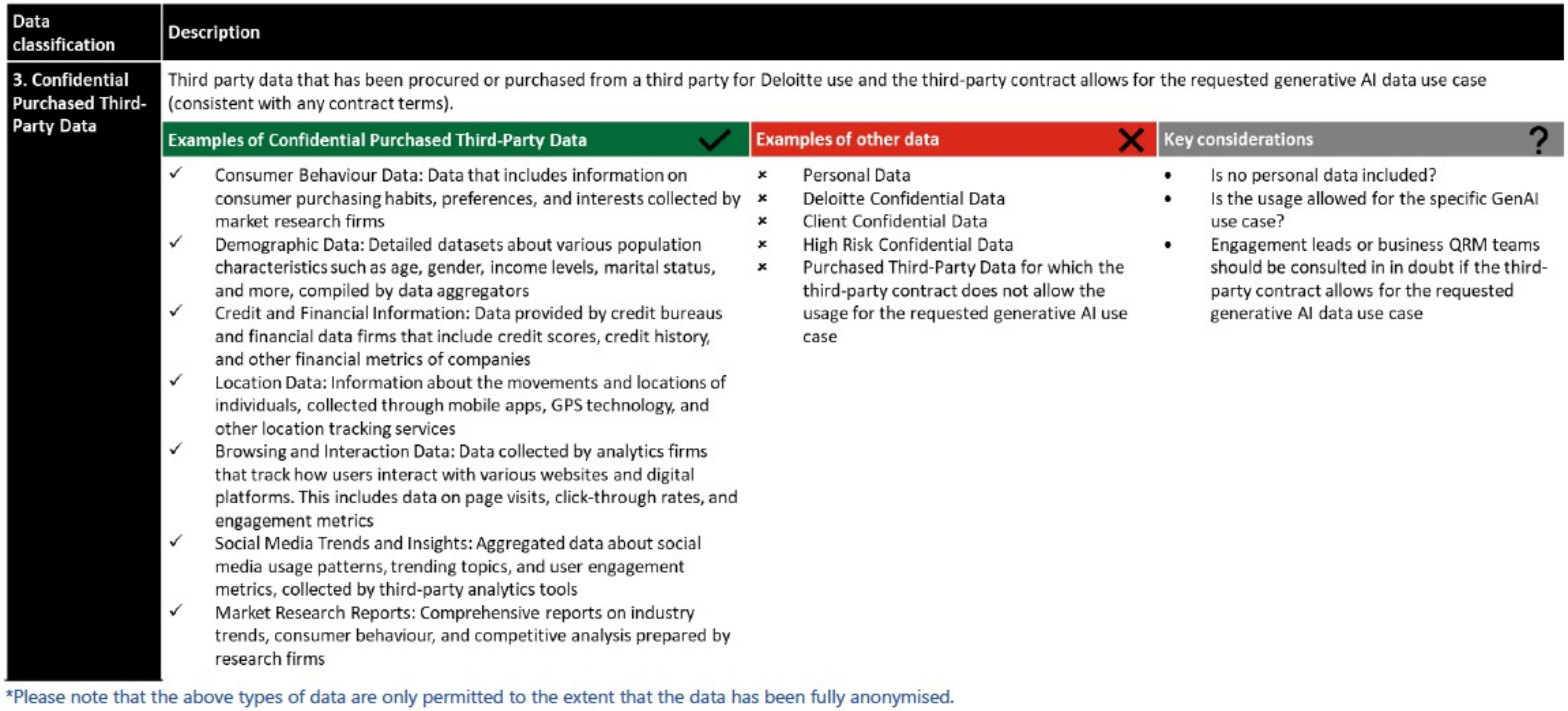


Appendix 2 – Data Guardrails: Confidential Data

Data classification	Description
2. Deloitte Confidential Data	Data not known to the public that relates to our business or that we receive in the course of business from other Deloitte personnel while it does not relate to our clients nor is obtained from third parties. This includes Business Contact data of Deloitte employees [1].

Examples of Deloitte confidential data ✓	Examples of other data ✗	Key considerations ?
✓ Deloitte developed templates and proposals, quals, and approaches (must exclude all client details) ✓ Deloitte external facing marketing materials ✓ Deloitte policies, procedures, and guidance documents ✓ Internal Deloitte business requirements/code ✓ Deloitte contract templates ✓ Deloitte training materials	✗ Board of Director minutes ✗ Deloitte's financial statements (unless these are made publicly available on the Internet) ✗ Deloitte firm pricing model materials and rate cards ✗ Individual level talent data ✗ Individual level employee activity ✗ Client Confidential Data ✗ Confidential Purchased Third-Party Data ✗ High Risk Confidential Data	• Does the data include client or third-party names or other client confidential data? • Does the data relate to Deloitte people and if so, considered Personal data that is out of scope?

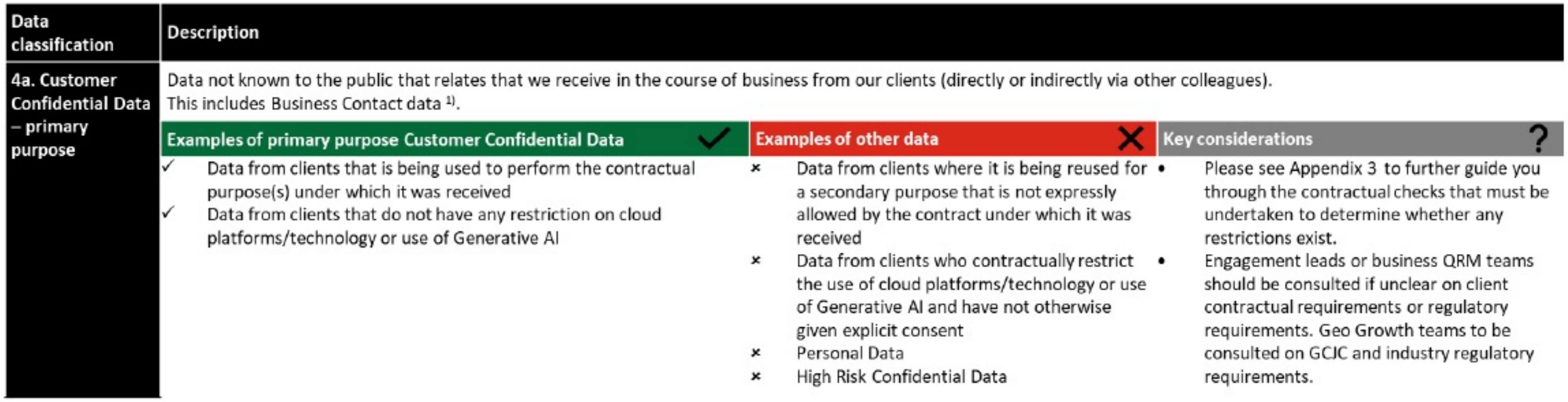
[1] An individual's name and one or more of the following business data: business name, title, role, address, telephone number (including mobile phone number) and e-mail address.



Data classification	Description		
3. Confidential Purchased Third-Party Data	Third party data that has been procured or purchased from a third party for Deloitte use and the third-party contract allows for the requested generative AI data use case (consistent with any contract terms).		
	Examples of Confidential Purchased Third-Party Data ✓	Examples of other data ✗	Key considerations ?
	✓ Consumer Behaviour Data: Data that includes information on consumer purchasing habits, preferences, and interests collected by market research firms ✓ Demographic Data: Detailed datasets about various population characteristics such as age, gender, income levels, marital status, and more, compiled by data aggregators ✓ Credit and Financial Information: Data provided by credit bureaus and financial data firms that include credit scores, credit history, and other financial metrics of companies ✓ Location Data: Information about the movements and locations of individuals, collected through mobile apps, GPS technology, and other location tracking services ✓ Browsing and Interaction Data: Data collected by analytics firms that track how users interact with various websites and digital platforms. This includes data on page visits, click-through rates, and engagement metrics ✓ Social Media Trends and Insights: Aggregated data about social media usage patterns, trending topics, and user engagement metrics, collected by third-party analytics tools ✓ Market Research Reports: Comprehensive reports on industry trends, consumer behaviour, and competitive analysis prepared by research firms	× Personal Data × Deloitte Confidential Data × Client Confidential Data × High Risk Confidential Data × Purchased Third-Party Data for which the third-party contract does not allow the usage for the requested generative AI use case	• Is no personal data included? • Is the usage allowed for the specific GenAI use case? • Engagement leads or business QRM teams should be consulted in in doubt if the third-party contract allows for the requested generative AI data use case

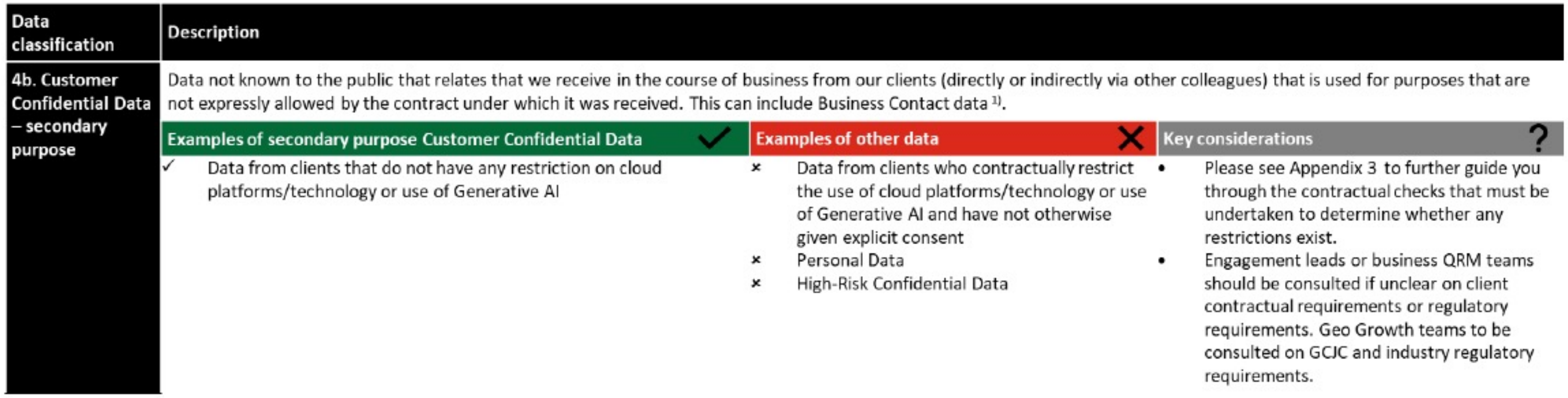
*Please note that the above types of data are only permitted to the extent that the data has been fully anonymised.

Deloitte.



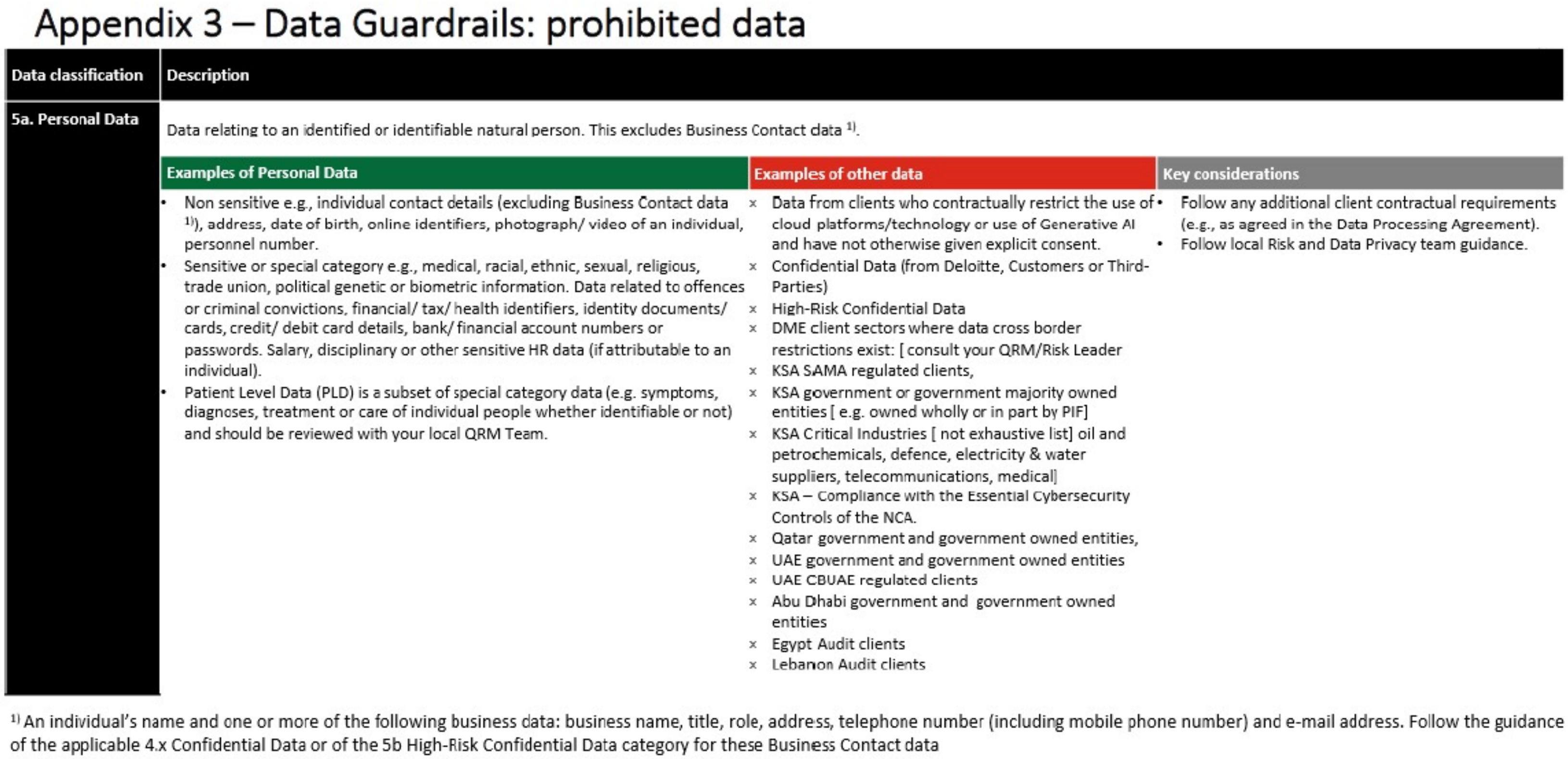
<table>
<tr><th>Data classification</th><th colspan="3">Description</th></tr>
<tr><td rowspan="3">4a. Customer Confidential Data – primary purpose</td><td colspan="3">Data not known to the public that relates that we receive in the course of business from our clients (directly or indirectly via other colleagues). This includes Business Contact data [1].</td></tr>
<tr><td>Examples of primary purpose Customer Confidential Data ✓</td><td>Examples of other data ✗</td><td>Key considerations ?</td></tr>
<tr><td>✓ Data from clients that is being used to perform the contractual purpose(s) under which it was received
✓ Data from clients that do not have any restriction on cloud platforms/technology or use of Generative AI</td><td>✗ Data from clients where it is being reused for a secondary purpose that is not expressly allowed by the contract under which it was received
✗ Data from clients who contractually restrict the use of cloud platforms/technology or use of Generative AI and have not otherwise given explicit consent
✗ Personal Data
✗ High Risk Confidential Data</td><td>• Please see Appendix 3 to further guide you through the contractual checks that must be undertaken to determine whether any restrictions exist.
• Engagement leads or business QRM teams should be consulted if unclear on client contractual requirements or regulatory requirements. Geo Growth teams to be consulted on GCJC and industry regulatory requirements.</td></tr>
</table>

[1] An individual's name and one or more of the following business data: business name, title, role, address, telephone number (including mobile phone number) and e-mail address.



<table>
<tr><th>Data classification</th><th colspan="3">Description</th></tr>
<tr><td rowspan="3">4b. Customer Confidential Data – secondary purpose</td><td colspan="3">Data not known to the public that relates that we receive in the course of business from our clients (directly or indirectly via other colleagues) that is used for purposes that are not expressly allowed by the contract under which it was received. This can include Business Contact data [1].</td></tr>
<tr><td>Examples of secondary purpose Customer Confidential Data ✓</td><td>Examples of other data ✗</td><td>Key considerations ?</td></tr>
<tr><td>✓ Data from clients that do not have any restriction on cloud platforms/technology or use of Generative AI</td><td>✗ Data from clients who contractually restrict the use of cloud platforms/technology or use of Generative AI and have not otherwise given explicit consent
✗ Personal Data
✗ High-Risk Confidential Data</td><td>• Please see Appendix 3 to further guide you through the contractual checks that must be undertaken to determine whether any restrictions exist.
• Engagement leads or business QRM teams should be consulted if unclear on client contractual requirements or regulatory requirements. Geo Growth teams to be consulted on GCJC and industry regulatory requirements.</td></tr>
</table>

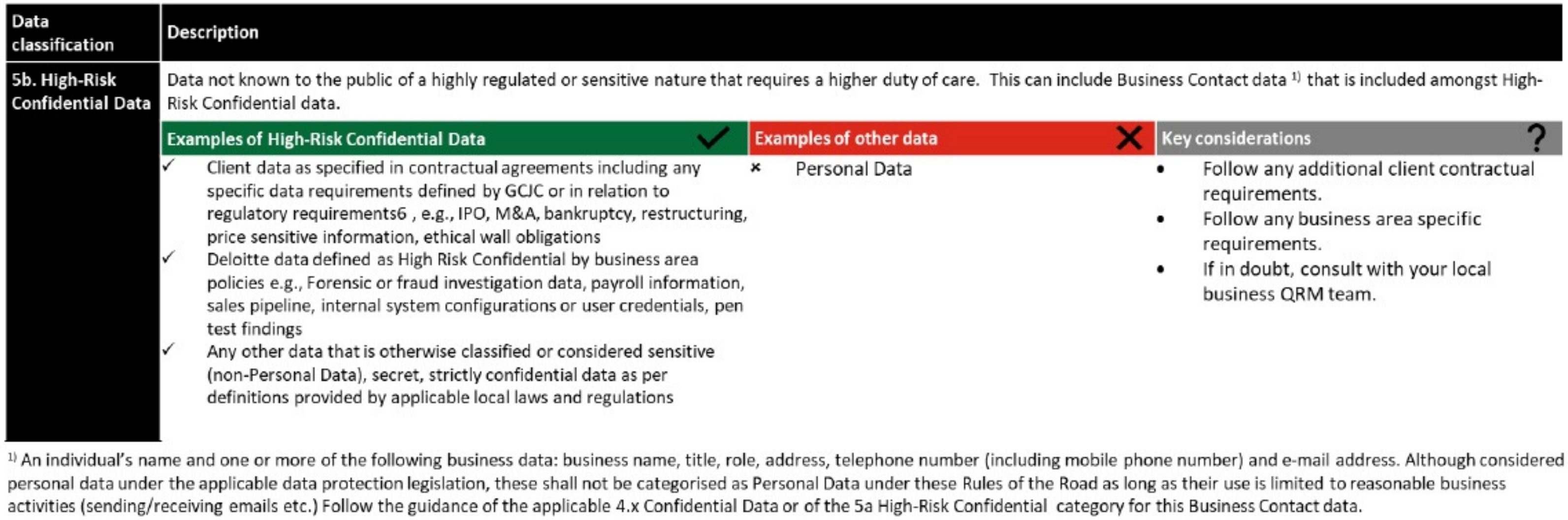
[1] An individual's name and one or more of the following business data: business name, title, role, address, telephone number (including mobile phone number) and e-mail address.



Appendix 3 – Data Guardrails: prohibited data

Data classification	Description		
5a. Personal Data	Data relating to an identified or identifiable natural person. This excludes Business Contact data [1].		
	Examples of Personal Data	Examples of other data	Key considerations
	• Non sensitive e.g., individual contact details (excluding Business Contact data [1]), address, date of birth, online identifiers, photograph/ video of an individual, personnel number. • Sensitive or special category e.g., medical, racial, ethnic, sexual, religious, trade union, political genetic or biometric information. Data related to offences or criminal convictions, financial/ tax/ health identifiers, identity documents/ cards, credit/ debit card details, bank/ financial account numbers or passwords. Salary, disciplinary or other sensitive HR data (if attributable to an individual). • Patient Level Data (PLD) is a subset of special category data (e.g. symptoms, diagnoses, treatment or care of individual people whether identifiable or not) and should be reviewed with your local QRM Team.	× Data from clients who contractually restrict the use of cloud platforms/technology or use of Generative AI and have not otherwise given explicit consent. × Confidential Data (from Deloitte, Customers or Third-Parties) × High-Risk Confidential Data × DME client sectors where data cross border restrictions exist: [consult your QRM/Risk Leader × KSA SAMA regulated clients, × KSA government or government majority owned entities [e.g. owned wholly or in part by PIF] × KSA Critical Industries [not exhaustive list] oil and petrochemicals, defence, electricity & water suppliers, telecommunications, medical] × KSA – Compliance with the Essential Cybersecurity Controls of the NCA. × Qatar government and government owned entities, × UAE government and government owned entities × UAE CBUAE regulated clients × Abu Dhabi government and government owned entities × Egypt Audit clients × Lebanon Audit clients	• Follow any additional client contractual requirements (e.g., as agreed in the Data Processing Agreement). • Follow local Risk and Data Privacy team guidance.

[1] An individual’s name and one or more of the following business data: business name, title, role, address, telephone number (including mobile phone number) and e-mail address. Follow the guidance of the applicable 4.x Confidential Data or of the 5b High-Risk Confidential Data category for these Business Contact data



Data classification	Description		
5b. High-Risk Confidential Data	Data not known to the public of a highly regulated or sensitive nature that requires a higher duty of care. This can include Business Contact data [1] that is included amongst High-Risk Confidential data.		
	Examples of High-Risk Confidential Data ✓	Examples of other data ✗	Key considerations ?
	✓ Client data as specified in contractual agreements including any specific data requirements defined by GCJC or in relation to regulatory requirements6 , e.g., IPO, M&A, bankruptcy, restructuring, price sensitive information, ethical wall obligations ✓ Deloitte data defined as High Risk Confidential by business area policies e.g., Forensic or fraud investigation data, payroll information, sales pipeline, internal system configurations or user credentials, pen test findings ✓ Any other data that is otherwise classified or considered sensitive (non-Personal Data), secret, strictly confidential data as per definitions provided by applicable local laws and regulations	× Personal Data	• Follow any additional client contractual requirements. • Follow any business area specific requirements. • If in doubt, consult with your local business QRM team.

[1] An individual's name and one or more of the following business data: business name, title, role, address, telephone number (including mobile phone number) and e-mail address. Although considered personal data under the applicable data protection legislation, these shall not be categorised as Personal Data under these Rules of the Road as long as their use is limited to reasonable business activities (sending/receiving emails etc.) Follow the guidance of the applicable 4.x Confidential Data or of the 5a High-Risk Confidential category for this Business Contact data.

Appendix 4 – Guidance to navigate Client Confidential Data

As with all technologies that our firm uses, we need to be mindful of the potential risks associated with these tools and approach them and their use in an ethical, confidential, private and secure way. Below is a summary, though not exhaustive view, of the risks that we need to consider and work through.

The following guidance will help you be sure that you are using Client Confidential Data (CCD) in Tax Genie 2.0 in line with the contractual purpose(s) under which it was received.

Scope

- Section 4a will assist you in reviewing the client contracts to determine whether any restrictions exist regarding the CCD you want to use in Tax Genie 2.0.
- Section 4b if necessary, this section will support you with obtaining explicit approval from the client(s) to use their CCD in Tax Genie 2.0 and explain how their data will be protected.
- Section 4c will help you to consider the data management aspects of the CCD you will input and create.

Section 4a - Contract reviews

These steps will help you review the relevant contract(s) that correspond to the CCD you want to enter into Tax Genie 2.0, so that you can confirm if the contract allows what you want to do or what action you may need to take if not:

1. Contact the LCSP for the client in question to check if an MSA guide is available, which may provide details on any restrictions relating to the use of CCD.

2. Clients may have requested all CCD is removed at the end of an engagement or there may be an obligation on Deloitte to do so when the contract comes to an end. We recommend you contact the Engagement Partner/Manager to make sure such a request was not made, as well as checking the relevant contract in accordance with point 3 below.

3. Check the terms and conditions of the contract under which the CCD was shared with Deloitte to establish the purposes for which Deloitte can use that CCD. The contract may be comprised of an overarching MSA or framework agreement, a SOW/Call-Off, an engagement letter, a change order for the GenAI addition that's a change to an existing SOW or engagement letter, an NDA signed with the same client and/or a combination of these. Key areas of focus of use limitations would be:
a. Confidential information clauses (including retention/destruction).
b. Intellectual property clauses.
c. Open-source clauses.
d. Exclusivity clauses.
e. Any references to models/machine learning/artificial intelligence.
f. Contents page.
g. Order of precedence clause (if multiple contractual documents to consider).

NOTE: 3 a-g above are suggestions only and there are likely to be other areas of the contract that address the use of CCD, so please read the contract(s) carefully and entirely before proceeding.

4. Document a summary of your checks and any consultations and retain a copy in your Engagement File.
5. If in any doubt, please consult with your Engagement leads or local Business area QRM teams.
6. Make sure that you have reviewed restrictions imposed via any potential CIMP controls. If in doubt speak to the Engagement Data Manager and/or the EP/LCSP.

Section 4b - Explicit client consent and how data is protected in Tax Genie 2.0.

If you need to, or to be transparent with the client about what you want to do, engage the LCSP and request that they connect with their counterpart at the client to approve the use of CCD being used in Tax Genie 2.0, noting:

- Our NSE Code of Conduct – where our principle of 'Integrity' requires that:
  - We are straightforward and honest in our professional opinions and business relationships.
  - We are truthful about the services we provide, the knowledge we possess, and the experience we have gained.

- You must not pass off works created by generative AI as your own. Clients will want assurance that we are not replacing Deloitte experience, skills and expertise with generative AI.
- Make sure to review carefully the relevant Terms of Business clauses of the Engagement Letter to verify that the client has accepted our reference to the possible use of GenAI by the engagement team in so far as to assist and formulate the potential deliverables [relevant clauses under preparation].

Explicit client consent should be obtained in writing from a client contact with relevant authority and filed in line with the data relating to the engagement (see Section 4c below).

The LCSP and/or engagement team will be able to correctly word and approach any such request; but we recommend that the request be written and include reference to the scope and purpose of the CCD use, along with reference to the relevant wording in the client contract that requires explicit consent to be obtained, following the requirements set out in the relevant client contract as a minimum.

If the client requires more information about Tax Genie 2.0 and how their data is protected then please use this guide to inform your discussion or talk them through via screen share, but please do not send the guide itself outside the firm.

If the review of the contract determines that use of the CCD in Tax Genie 2.0 for the intended purpose is not allowed, but the engagement team and LCSP together determine that they will request client consent to do so anyway, then in addition to the approach discussed above, the client contract would have to be varied in accordance with the terms of that contract.

Section 4c - Data Management considerations

In addition to confirming contractually if client (confidential) data can be used or getting the client's clear consent to use their data within Tax Genie 2.0, you will also need to think about how to manage the data that you plan to input into Tax Genie 2.0 as well as the content that is created by Tax Genie 2.0:

1. Store all data (including the CCD planned for use in the engagement) and any outputs generated from Tax Genie 2.0 in line with your local data storage requirements.

2. Ensure that this specifically created folder is only accessible to the relevant people who are part of the engagement team, and that any generated output is not to be shared outside of the engagement.

3. Make sure that the CCD is classified as Confidential using the file's editing app's built-in classification tool.

4. Store a copy of any output generated from Tax Genie 2.0 using CCD in the corresponding folder from where the input CCD was taken, if possible, depending on use case.

5. No originating CCD or Tax Genie 2.0 outputs are to be stored anywhere other than the repositories as described above, i.e. ensure there are no copies on your desktop or OneDrive.

6. Make sure that the output/copy of the output is classified as Confidential using the file's editing app's built-in classification mechanism AIP, and check it is in line with your local data classification policy and that the classification has not been upgraded. If so, reclassify as appropriate.

7. Delete all CCD input and the output generated by Tax Genie 2.0 from within the Tax Genie 2.0 platform at the end of the engagement.