VERIFICATION CODE

AM$

FOR CLE CREDIT:

1. Write down or take a photo of this Verification Code.

You **MUST** complete the evaluation to earn CLE Credit.

2. Either click the "Evaluation" button from the program on your **Meeting App** to enter the Verification Code and complete the Program Evaluation now.

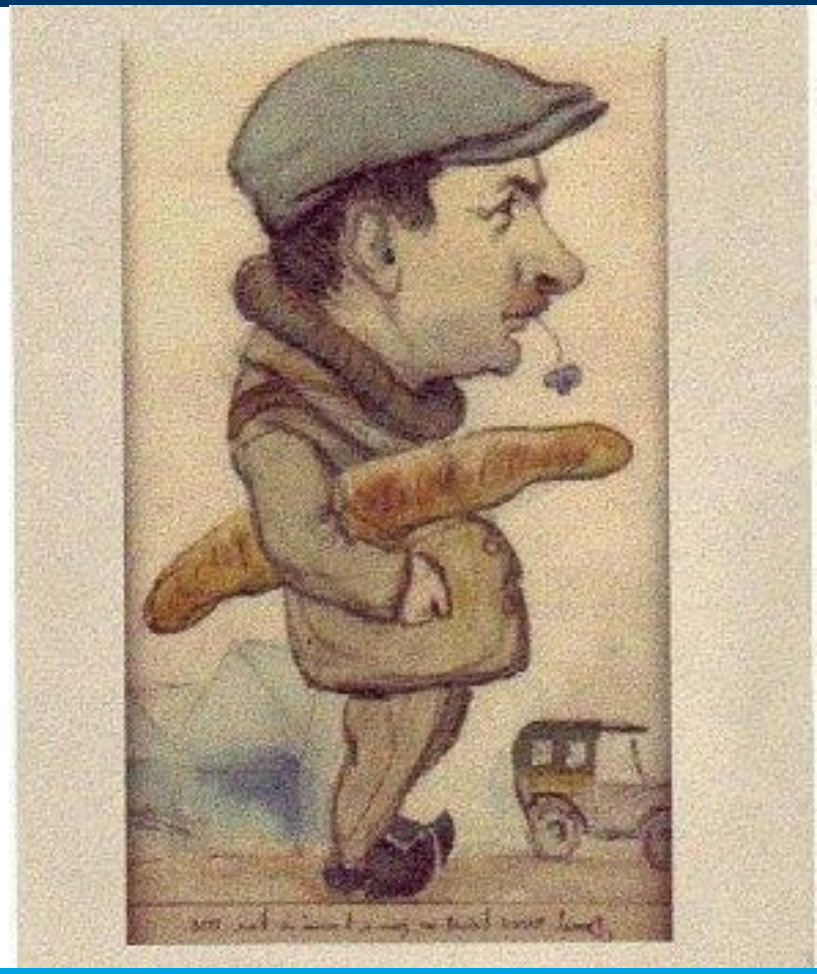
OR

3. Save the code to take the evaluation later.

We Do Not Like Discovery / Disclosure!

Judgment of the Marseilles Civil Court of February 20, 1974

"*It appears, clearly, that one can not impose one of the litigants, against his will, to communicate all of the documents, certificates, personal papers, correspondence, received or otherwise, that it could hold in its files, binders, cases or boxes, without knowing first which documents they could be and if they could present a connecting link with an element of proof for the case; that acting inquisitorially against one of the parties to call upon it to present for everyone to see documents which cannot be determined and are not determined, with the sole intention of allowing the opposing party to look through them to possibly search for an element of proof that it is not certain to obtain would seriously harm the individual freedom that all litigants have the right to assert.*"



- French Law no. 68-678 of 26 July 1968
- Article 271 (1) of the Swiss Criminal Code

- Passed to regulate the use by U.S. and English courts (mainly) of the Discovery/Disclosure procedure (request for documents to be communicated)
- The purpose of the Evidence Law is:
  - ✓ To protect sensitive information and data harming the interests of France and its companies, that could be provided as evidence in the scope of legal proceedings abroad
  - ✓ To compel foreign authorities to comply with international mutual legal or administrative assistance channels
- **Criminal penalties:** the seeking of and the communication by a company, as well as by its employees or managers, of information that violates the Evidence Law is punishable by six months' imprisonment and an 18,000 Euro fine (x5 for a legal entity)
- But led to **very few legal proceedings in France** → limited efficiency (so far) when it is invoked before foreign courts
- Recent reform of the Evidence Law to grant it more credibility before foreign courts

- **Mission:** Ensure the Evidence Law is applied by the people who are subject to it – legal safety + single spokesperson for companies
- Decree no. 2022-207 (Evidence Law reform) → **New missions granted to the SISSE:**
  - Obligation for companies to immediately inform it in the event of a request for documents to be communicated before foreign courts
  - Power to issue opinions (one month period from the application to the SISSE) regarding the application of Articles 1 and 1bis of the Evidence Law to help companies identify the data that can be sent:
    - Article 1 – only for data that would be both "company sensitive" and "sovereign sensitive"
    - Article 1a – broader scope because it concerns all "*economical, commercial, industrial, financial or technical*" information + requires the use of the transmission mechanisms provided for in the Hague Convention of 18 March 1970 applicable to judicial cooperation between FR and the UK
- A non-binding opinion but that can be provided to support a refusal to communicate documents before foreign courts to reinforce the credibility of the developed defence

Application to the SISSE

Inform it of the disclosure requests received in the scope of the foreign proceedings

Request an opinion regarding:

- the application of Article 1 – Identify the data that are “company sensitive” and “sovereign sensitive” that are not likely to be sent
- the application of Article 1bis – requires using the transmission mechanisms that are provided for in the Hague Convention

Benefit from support and guidance from the State regarding the defence developed abroad

- Regulation 216/679
- GDPR replaced the data protection directive (Directive 95/46/EC).
- GDPR was designed to harmonize data privacy laws across Europe, to protect and empower the data privacy of all EU citizens and to reshape the way organizations across the region approach data privacy
- Entered into force on **25 May 2018**

1. the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not
2. the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    b. the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law

Personal Data

Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject

Means the natural person identified or identifiable through the Personal Data.

Processing

Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Transfer

Means the disclosure of Personal Data to a third party by (i) transferring the data to the third party or (ii) the third party inspecting or retrieving data available for inspection or retrieval.

Controller

Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Special Categories of Personal Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

1. Personal data shall be:
    a. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
    b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … (‘purpose limitation’);
    c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
    d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
    e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed … (‘storage limitation’);
    f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)

- Processing shall be lawful only if and to the extent that at least one of the following applies:
  a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (See Art. 7 GDPR)
  b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  c. processing is necessary for compliance with a legal obligation to which the controller is subject;
  d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

- The *transfer* of Personal Data across national borders is only permissible if the recipient country and/or the recipient ensures an appropriate level of protection (Art. 44 GDPR):
  - **Transfers on the basis of an adequacy decision (Art. 45 GDPR)**
  - **Transfers subject to appropriate safeguards (Art. 46 & 47 GDPR)** – e.g., binding corporate rules, standard data protection clauses
  - **Derogations for specific situations (Art. 49 GDPR)**

Countries Providing an Adequate Level of Data Protection – 40

- European Union Member States – 27:
- Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain & Sweden

- Third Countries – 13
- Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, United Kingdom under GDPR and LED, United States (limited to Privacy Shield framework), & Uruguay

- In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

  a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

  b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

  c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;

e. the transfer is necessary for the establishment, exercise or defence of legal claims;

f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Infringements shall be subject to administrative fines up to €10 million / €20 million, or in the case of an undertaking, up to 2% / 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

- All testimony must be given voluntarily without coercion or threat of future sanctions
- All depositions in Germany must take place at the U.S. Consulate General in Frankfurt
- Bilateral agreements between Germany and the United States require that the German Ministry of Justice pre-approves all requests for depositions
- Depositions taken without the prior approval of the German Ministry of Justice and/or without the involvement of the United States Mission to Germany are unauthorized and may lead to criminal penalties against the participants
- Under the provisions of bilateral agreement(s), U.S. Consular Officers in Germany have the right to administer depositions only in civil cases. Depositions related to criminal cases are accomplished via letters rogatory

1. https://de.usembassy.gov/judicial-assistance/
2. https://de.usembassy.gov/wp-content/uploads/sites/19/2024/03/Deposition-Instructions-2024.pdf

Blocking Statutes—The American Way:

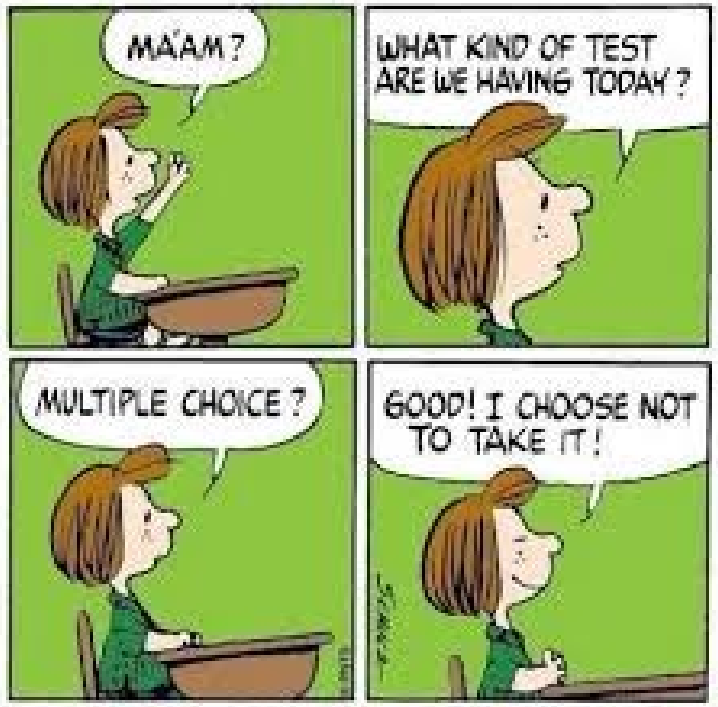
Blocking Statutes—The American Way:

- The United States is a signatory to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters.
- Societe Nationale Industrielle Aerospatiale v. U.S. District Court, 482 U.S. 522 (1987) announced the standards that United States courts should follow when a party's discovery obligations in U.S. litigation present a potential conflict with its obligations under foreign laws.

Societe Nationale Industrielle Aerospatiale v. U.S. District Court, 482 U.S. 522 (1987):

- The Hague Evidence Convention does not provide exclusive or mandatory procedures for obtaining discovery in international territories.
- Use of the Hague Procedures constitutes an option depending on scrutiny of the particular facts, sovereign interests, and likelihood of success.

Courts applying Aerospatiale:



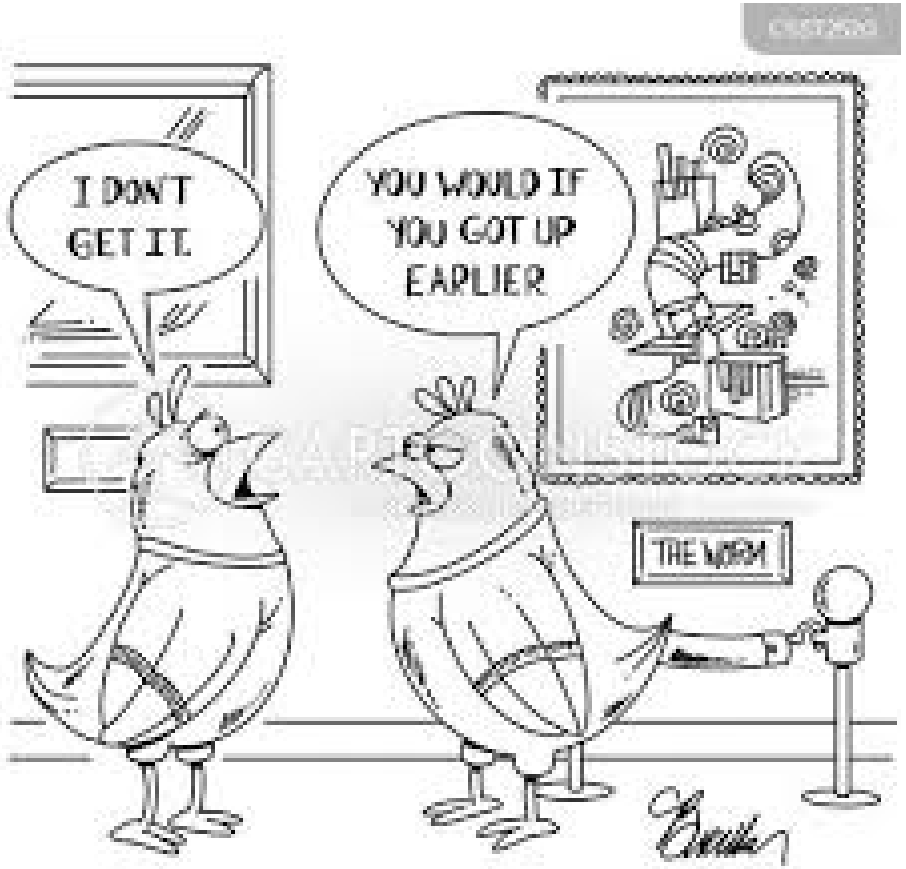
- Three-Factor Test;
- Four-Factor Test;
- Five-Factor Test; and
- Seven-Factor Test.

Courts applying Aerospatiale:

- Importance of the information requested to the case;
- Specificity of the request;
- Location of the information;
- Availability of alternative means of securing the information;
- Competing national interests;
- Hardship to international litigant; and
- Likelihood of compliance.

Practically speaking:

- Start early;
- Demonstrate good faith; and
- Be prepared to educate the court about the different procedures under the Hague.



Because remember:

As the court in Salt River Project Agricultural Improvement & Power Dist. v. Trench France SAS, 303 F. Supp. 3d 1004 (D. Ariz. 2018) said:

> The Supreme Court has explained that use of Hague Procedures is "optional," and that "the Hague Convention did not deprive the District Court of the jurisdiction it otherwise possesse[s] to order a foreign national party before it to produce evidence physically located within a signatory nation." Aerospatiale, 482 U.S. at 539–40. Even where ordering the foreign party to produce discovery will potentially cause the party to violate a blocking statute in its home country, use of Hague procedures is not mandatory. Id.; see also Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1471 (9th Cir. 1992).

Blocking Statutes—The Canadian Way:

> "*In an ever-shrinking world, Canadian courts often require the assistance of foreign courts so as to do justice between parties engaged in litigation in Canada. A receptive judicial ear to requests from foreign courts can only enhance the chances that a Canadian court will receive assistance when required*."[1]

- Canadian courts seek to accommodate reasonable requirements of foreign laws so long as it does not unduly compromise the fact-finding process and it is within the bounds Canadian sovereignty to do so

[1] *France v. De Havilland Aircraft of Canada Ltd. (1991), 3 O.R. (3d) 705 (C.A.)*

Frischke v. Royal Bank of Canada (1977), 17 O.R. (2d) 388 (C.A.)

- alleged misappropriation of funds by defendants
- plaintiff applied to add Canadian bank as party to trace funds
- plaintiff applied for injunctive order compelling bank to disclose information of payments from its branch in Panama
- personnel at Panama branch refused because disclosure would breach banking secrecy laws of Panama

Frischke v. RBC

Ontario Court of Appeal: **Held** – reversed order of motion court which had compelled disclosure by Panamanian bank personnel:

> "*An Ontario Court would not order a person here to break our laws; we should not make an order that would require someone to compel another person in that person's jurisdiction to break the laws of that State. We respect those laws. The principle is well recognized*."

Not a hard and fast rule; case by case assessment

e.g. *R. v. Spencer (1983), 145 DLR (3d) 344 (Ont. C.A.), aff'd [1985] 2 SCR 278*

- criminal case
- Crown served subpoena on individual who, 10 years earlier, had served as manager of a branch of Canadian bank in Bahamas
- individual applied to quash subpoena on ground Bahamian banking secrecy laws prohibited him from disclosing information obtained in his capacity as manager of bank branch
- motion judge quashed subpoena
- Crown appealed

R. v. Spencer – Ont. C.A.:

- reversed motion decision; held information must be disclosed
- paramount public policy consideration-- “the basic principle that the parties and the public have the right to every person's evidence”
- while international comity as recognized in *Frischke* is important, it could not be applied so as to override this right
- appeal to Supreme Court of Canada

R. v. Spencer

- SCC affirmed Ont. C.A.'s decision
- LaForest, J.:

  "*To allow Mr. Spencer to refuse to give evidence in the circumstances of this case would permit a foreign country to frustrate the administration of justice in this country in respect of a Canadian citizen in relation to what is essentially a domestic situation. Indeed such an approach could have serious repercussions on the operation of Canadian law generally*."

- Concurring reasons of Estey J. gave greater weight to considerations of comity:

  "*The fact that the giving of the evidence sought in this case may constitute a crime in another country cannot prevent the Canadian courts from compelling a witness to testify. However, the threat arising in a foreign jurisdiction of criminal proceedings against a Canadian resident for revealing information in a Canadian judicial proceeding is a serious consideration to be borne in mind in a proceeding such as this. Thus, any course by which such a serious consequence may be avoided must be carefully considered by our courts. In these proceedings it is therefore relevant to take note of the fact that under Bahamian law an appropriate order releasing the appellant may be obtained from a Bahamian court.*

  …

  It therefore would have been a preferable alternative at the trial level to have granted a stay of these proceedings so as to allow the appellant sufficient time to make application to a Bahamian court of competent jurisdiction for an order permitting disclosure of the evidence sought to be compelled".

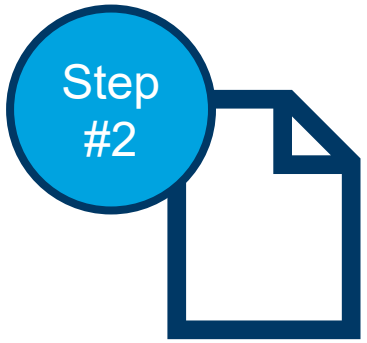
GDPR:
Harris v Bayerische Motoren Werke Aktiengesellschaft, 2022 ONSC 6435; aff'd 2024 ONSC 2341 (Div. Ct.)

- BMW defendant in lawsuit
- applied for directions that it be permitted to produce its documents in a manner that would comply with GDPR
- adduced expert evidence of German law:
  1. use of personal data for purpose of asserting or defending against a lawsuit is a "legitimate interest" which constitutes an exemption to disclosure restrictions;
  2. two factors for applying Legitimate Interest exemption: (a) is the specific data in the document necessary for advancing/defending claim? and (b) does interest of the party to the lawsuit who needs disclosure of the personal data outweigh interest of affected person in preserving privacy of the personal data?

Harris v. BMW AG

- BMW's expert evidence: "layered approach" – i.e., produce documents in two steps:

Produce all documents with all personal data reacted



Subsequently "unredact" if it is determined that personal data in a given document is necessary for either plaintiff or defendant to assert/defend the claim

Harris v. BMW AG: Motion Judge (Perell, J.)

- Plaintiff opposed redaction entirely;
- Held in favour of BMW
- Judge found both “necessity” and “balancing of interests” requirements are “baked into” Ontario court rules
- BMW is to initially review each document, and may redact personal data from its documents to comply with GDPR if:
  1. data are not relevant to issues in lawsuit; and
  2. disclosure would cause significant harm to BMW or would “infringe public interests deserving of protection”, which includes interest of person to whom the personal data relates.
- Plaintiff appealed

Harris v. BMW AG: Ontario Divisional Court

- Plaintiff appealed.
- Divisional Court dismissed plaintiff's appeal:

  "…this is a matter of international comity; while foreign laws cannot dictate the procedures to be followed by Canadian courts, a foreign litigant should not be compelled to contravene the laws of its jurisdiction if domestic fact-finding process can accommodate compliance with foreign laws."

Conclusion

- The Canadian Way -- Respect for international judicial comity:
- Accommodate foreign laws either by giving foreign party opportunity to seek from its own courts relief from the obligations imposed by the foreign law, or by crafting a solution within the available framework of Canada's laws and rules of court.

VERIFICATION CODE

AM$

FOR CLE CREDIT:

1. Write down or take a photo of this Verification Code.

You **MUST** complete the evaluation to earn CLE Credit.

2. Either click the "Evaluation" button from the program on your **Meeting App** to enter the Verification Code and complete the Program Evaluation now.

OR

3. Save the code to take the evaluation later.