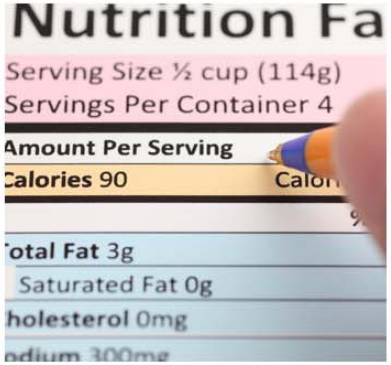

feeding the minds that feed the world

# Section Leader Webcast:
# Sections, Data Privacy and Data Processing Agreements
# February 20, 2019

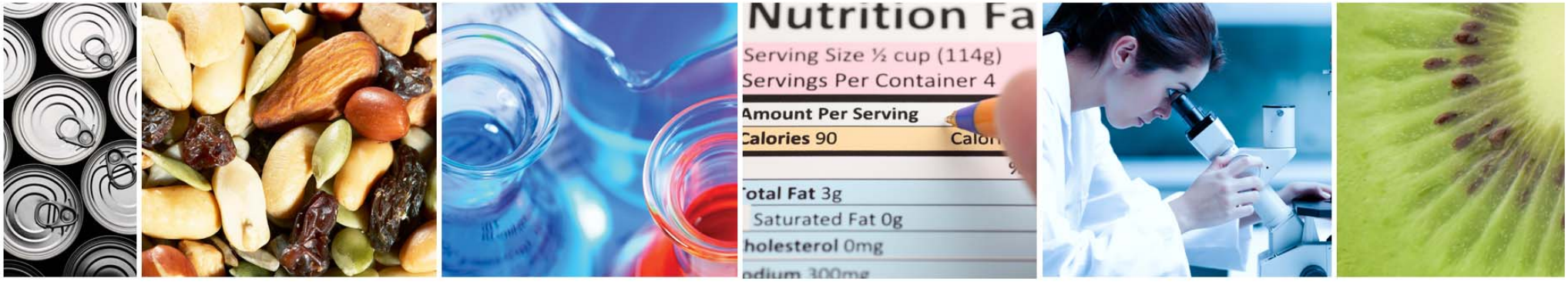



# Institute of Food Technologists

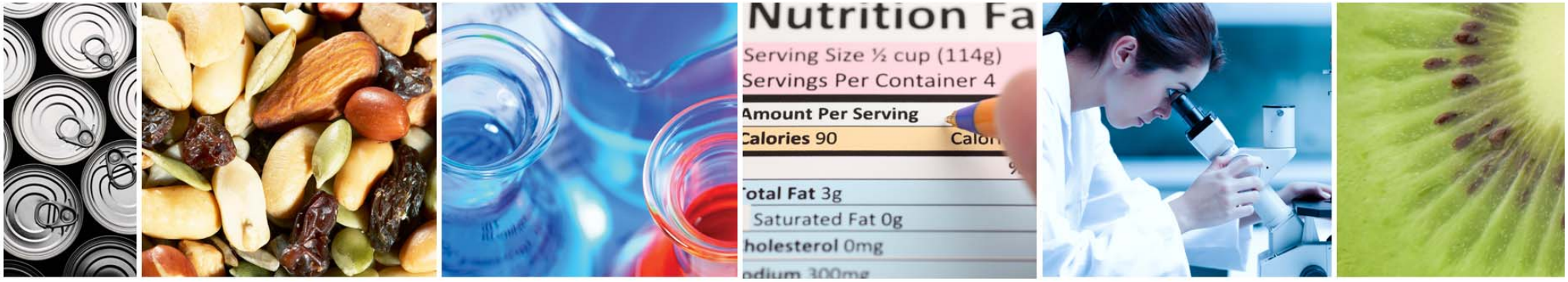
**Tom Foley**
*VP, Membership & Customer Development*

**Terry Merkley, MBA**
*Vice President, Information Technology*




# Agenda

- Welcome - Introductions
- GDPR Refresher
- Introduction to DPAs
- DPAs for Sections
- Section Vendor DPAs
- Wrap-up/Next Steps/Resources



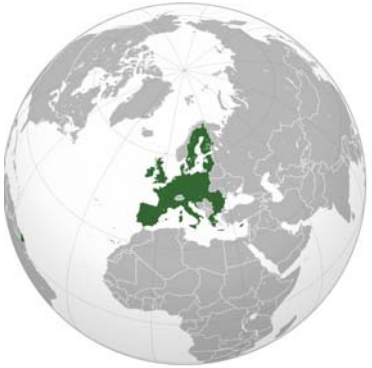

# GDPR Refresher

# What is GDPR?

- Developed by the European Commission to strengthen and unify data privacy protection across the EU.
- Approved in 2016; Enforceable (worldwide) as of May 25, 2018.
- Includes specific provisions for the handling of personal data of EU data subjects that are exported outside the EU.
- Imposes mandatory reporting for data breaches, duty to respond to EU citizens' privacy rights, increased sanctions for noncompliance, revised consent criteria, and much more.
- Subjects all organizations that maintain and use European member or customer data to these regulations.

# Common GDPR Questions

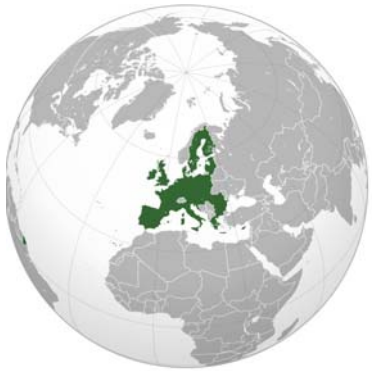
- Who does the GDPR affect?
- How does the GDPR affect policy surrounding data breaches?
- What are the penalties for non-compliance?
- What are my responsibilities?
- What are all these GDPR terms like a data processor and a data controller?



Source: https://upload.wikimedia.org/wikipedia/commons/7/73/Global_European_Union.svg

# Who is Affected by GDPR?

- GDPR applies not only to organizations located within the EU but also to organizations located outside of the EU if they offer/provide goods or services to EU data subjects.
- It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.



Source: https://upload.wikimedia.org/wikipedia/commons/7/73/Global_European_Union.svg

# Key Principles of GDPR

- Data subjects own their personal data
- Organizations should keep only the personal data they need, only for as long as they need it, and only for the purposes indicated in their lawful basis.
- Data subjects have the right to request changes to the way an organization uses their personal data
- Organizations must respond to such requests in a timely way

# Major Requirements for Organizations

- Effective information security controls
- Rapid breach notification plan
- Maintain record of personal data processing activity
- Maintain record of requests from data subjects to alter or remove their personal data
- Conduct data privacy assessments for new initiatives
- More…

# Penalties for Non-Compliance

- GDPR imposes stiff fines on data controllers and processors for non-compliance.
- Fines vary based on the severity of non-compliance. The most significant penalties are up to €20 million, or 4% of the organization's annual revenue, whichever is higher.

# We Don’t Have Members In The EU….Does This Apply?

- **Regardless of GDPR requirements, many of the items we are discussing today involve best practices when handling member data!**
- **We also anticipate more regulations could be put in place domestically with restrictions similar to GDPR.**

  - *June 28, 2018: New York Times:*
    *California Passes Sweeping Law to Protect Online Privacy*

    *“California has passed a digital privacy law granting consumers more control over and insight into the spread of their personal information online, creating one of the most significant regulations overseeing the data-collection practices of technology companies in the United States……The legislation, which goes into effect in January 2020, makes it easier for consumers to sue companies after a data breach. And it gives the state’s attorney general more authority to fine companies that don’t adhere to the new regulations.”*

# Top 5 Things for Sections To Do…..

1. Understand who has access to your data

2. Understand your data!
   - What is being collected?
   - How is it being processed?
   - Is it necessary to business functions?

3. Have a compliance plan that shows steps you intend to take
   - Establish Data Processing Agreements that define responsibilities and protections for personal data you provide to other organizations
   - Document your activities as you move forward with your plan

# Top 5 Things for Sections To Do…..

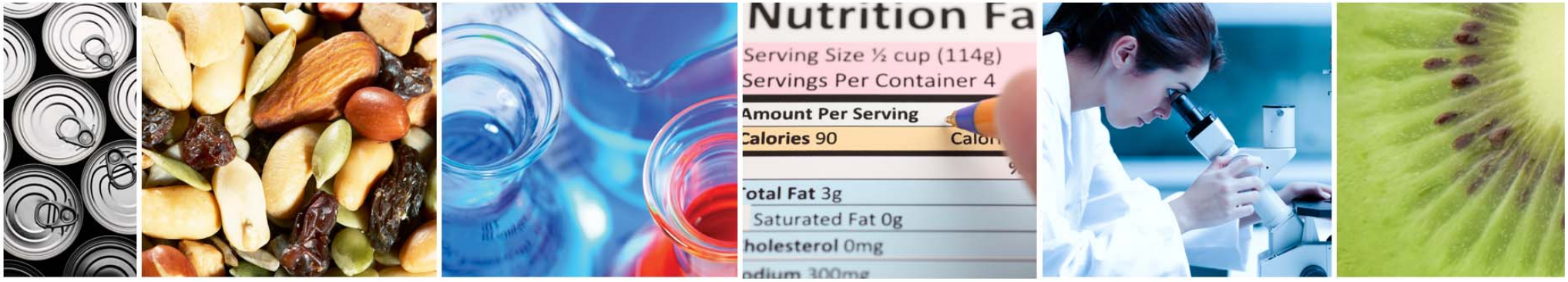
4. Talk to your vendors - Understand how they use your data

5. Follow-up immediately with members who request to be forgotten or have specific questions on GDPR

# Additional Resources

**Here are some additional resources where you can learn more about IFT's Privacy Policy & GDPR:**

- IFT Privacy Policy
  http://www.ift.org/About-Us/Privacy-Policy.aspx
- Forbes - *Three strategic realities for CIOS as the GDPR Deadline Draws Near*
  https://www.forbes.com/sites/forbestechcouncil/2018/01/24/three-strategic-realities-for-cios-as-the-gdpr-deadline-draws-near/#1e32ccbbb806
- ASAE/Associations Now: 4 Data Issues TO Act On Now, As GDPR Looms
  https://associationsnow.com/2018/03/4-data-issues-to-act-on-now-as-gdpr-looms/
- EU GDPR Informational Portal
  https://www.eugdpr.org/
- IHasco GDPR Essential Online Training:
  https://www.ihasco.co.uk/courses/detail/gdpr-training




# Introduction to DPAs

# Controllers and Processors

**Q:** What is a Controller?

**A:** An organization that determines what personal data will be collected along with the purposes and means of processing personal data

**Q:** What is a Processor?

**A:** An organization that is responsible for processing personal data on behalf of and under the direction of a Controller

**Q:** What is being controlled and processed?

**A:** Data that can uniquely identify residents of the European Union

# Shared Responsibility

**Q:** Which party is responsible for complying with GDPR?

**A:** It is a shared responsibility among Controllers and Processors

**Q:** Is responsibility shared 50% - 50%?

**A:** In general, responsibility likely rests more heavily on Controllers because they determine the purposes and means of processing

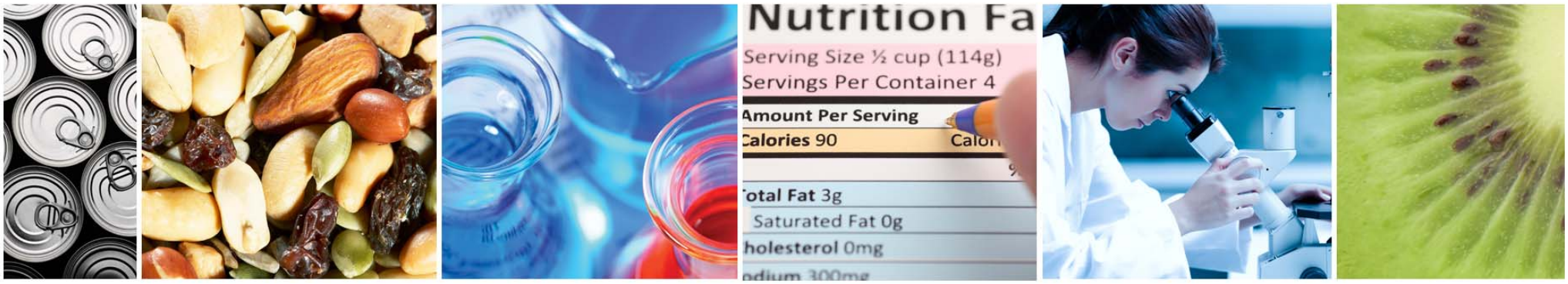
**Q:** What is the best way to agree on how responsibility is shared?

**A:** With a Data Processing Agreement (DPA)

# What is a DPA?

**Q:** What is a DPA?
**A:** A DPA is a legal contract between Controller and Processor

**Q:** What does a DPA establish?
**A:** Which party is the Controller; which is the Processor
**A:** Which data will be processed, incl. any special data
**A:** What processing is to be done
**A:** The purpose(s) for the data processing
**A:** Any subprocessors the Processor may use
**A:** Obligations (and their limits) on Controller and Processor
**A:** Specific obligations that would arise from a data breach
**A:** Mutual indemnifications




# DPAs for Sections

# Duty of Care

- The Section Board of Directors has a fiduciary duty to the organization, including duties of care, loyalty, and obedience. **Section directors are required to act reasonably, prudently, and in the best interests of the organization**; to avoid fraud and negligence; and to avoid conflicts of interest.
- No loans shall be contracted on behalf of the section, and no negotiable papers, other than checks, are issued in its name, unless and except as authorized by a majority vote of the Section Board of Directors.
- All funds of the section shall be deposited to the credit of the section in such depositories as the Board of Directors may select. All funds of the section, except for investment accounts, shall be in depositories covered by the Federal Deposit Insurance Corporation and shall be withdrawn according to procedures prescribed by the Section Board of Directors.

**IFT SECTION AFFILIATION AGREEMENT**
**DATA PROCESSING AGREEMENT ADDENDUM**

1. Introduction – This Data Processing Agreement ("**DPA**") is entered into on [insert date] by and between Institute of Food Technologists (IFT, hereafter) and XXXX Section IFT This DPA reflects the parties' agreement with respect to the terms governing the processing of Personal Data resulting from the activities described in the XXXX Section IFT Affiliation Agreement dated {insert date] (the "**Agreement**"). The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement or the General Data Protection Regulation ("**GDPR**") (Regulation (EU) 2016/679).

2. This DPA Includes –

   2.1. EXHIBIT 1 - Personal Data Processing
   2.2. EXHIBIT 2 – List of Subprocessors (Section Vendors)

3. Roles of the Parties –

   3.1. Controller – IFT is the public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data within the context of the performance of the Agreement and is deemed a "**Controller**" within the meaning of the GDPR.
   3.2. Processor – XXXX Section IFT., which processes Personal Data on behalf of the Controller and within the context of the performance of the Agreement, is deemed a "**Processor**" within the meaning of the GDPR.

4. Personal Data - Processor anticipates that in the course of serving as a section of IFT, and performing activities governed by the sections Affiliation Agreement., Processor may receive or have access to the Personal Data of European Union individuals. Processor agrees to comply with the provisions of this DPA with respect to all Personal Data processed for Controller in connection with the Agreement. "**Personal Data**" means any information about an identified or identifiable individual, including a name, address, email, phone number, photo, location data, and any other data which may relate to the identification of a person. The Personal Data that the parties anticipate will be processed pursuant to this DPA are provided on the attached **Personal Data to be Processing**, attached hereto as **EXHIBIT 1**.

5. Compliance - Processor, on behalf of its volunteers, contractors, subprocessors, partners and affiliates, represents and warrants that it will handle all Personal Data in compliance with all applicable data protection laws including, but not limited to, EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR, as well as to the data protection or privacy laws of any other country (collectively "**Data Protection Laws**").



6. Obligations of Controller - Controller shall, in its performance under the Agreement, process Personal Data in accordance with the requirements of Data Protection Laws and Controller will ensure that its instructions for the processing of Personal Data shall comply with Data Protection Laws. Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data, the means by which Controller acquired Personal Data, and meeting all requirements and legal responsibilities necessary to process the Personal Data, and transfer or allow access to the Personal Data to Processor.

7. Obligations of Processor – Processor specifically agrees to meet its obligations as a data processor under GDPR, including GDPR Articles 28-37 and requirements regarding restrictions on subprocessors, maintaining records of processing activities, and implementation of measures to assist Controller in responding to and complying with the rights of data subjects, data security, and data breach reporting. Processor shall collect, process and use Personal Data only within the scope of sections affiliation agreement and shall treat Personal Data as confidential information. Processor shall appoint a Data Protection Officer, if this is legally required and, upon request of Controller, Processor shall notify Controller of the contact details of the appointed individual. Processor must ensure that any Personal Data that it processes are kept confidential. To the extent possible, Processor shall limit access to Personal Data to those Processor volunteers, subprocessors or contractors who need to know/access the relevant Personal Data only for the purposes of performing its obligations under this Agreement and that such persons are subject to confidentiality obligations regarding the same. Processor shall either return or destroy all Personal Data at the termination of its agreement with Controller as described in paragraph 12. Processor shall provide Controller with all information necessary to demonstrate Processor's compliance with GDPR upon Controller's request.

8. Subprocessors - Controller acknowledges and agrees that Processor may engage third party sub processers and that Processor and Processor's affiliates respectively may engage third-party subprocessors in connection with performance under the Agreement. Any such subprocessors shall be permitted to obtain Personal Data only to deliver the services Processor has retained them to provide, and they are prohibited from using Personal Data for any other purpose. Processor acknowledges and agrees it shall be liable for the acts and omissions of its subprocessors to the same extent Processor would be liable if performing the services of each subprocessor directly under the terms of this DPA, except as may be otherwise set forth in the Agreement. The subprocessors that the parties anticipate will be engaged relevant to the processing of Personal Data relating to this DPA are provided on the attached **List of Subprocessors (i.e. section vendors, including section administrators)**, attached hereto as **EXHIBIT 2**. Processor shall notify Controller in writing of any relevant changes or additions to its subprocessors.

9. Rights of Data Subjects - To the extent Controller does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, Processor

shall comply with any commercially reasonable request by Controller to facilitate such actions to the extent Processor is legally permitted to do so. To the extent legally permitted, Processor shall promptly notify Controller if it receives a request from a data subject for access to, correction, amendment, or deletion of that individual's Personal Data and Processor shall provide Controller with commercially reasonable cooperation and assistance in relation to handling of a data subject's request. Processor shall not respond to any such data subject request without Controller's prior consent except to confirm that the request relates to Controller.

10. Security - Processor shall, in relation to Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. To learn more visit: www.gdpr-info.eu.

11. Breach of Personal Data - Processor shall notify Controller without undue delay upon Processor or any subprocessor becoming aware of a breach of Personal Data, providing Controller with sufficient information to allow Controller to meet any obligations to report or inform the individuals whose Personal Data has been breached in compliance with Data Protection Laws. Processor shall cooperate with Controller and take such reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such breach of Personal Data.

12. Deletion or Return of Personal Data - Upon termination or expiration of this Agreement, Controller shall advise Processor as to whether Processor shall delete or return Personal Data. Upon receipt of such notice, Processor shall comply with Controller's directive promptly and confirm to Controller when the directive has been completed.

13. Indemnification - Processor shall indemnify, defend and hold Controller, its officers, directors, employees, agents, and each of them ("Indemnitees"), harmless against all claims, actions, third party claims, losses, harm, costs, fines, liability, damages and expenses incurred by Controller and arising directly or indirectly out of or in connection with a breach of this Agreement and/or applicable Data Protection Laws by Processor.

14. Privacy Policy – Processor agrees to adhere to IFT's Privacy Policy, which can be found here: http://www.ift.org/about-us/privacy-policy.aspx

**Agreed to by:**

**INSTITUTE OF FOOD TECHNOLOGISTS**
**[CONTROLLER]**
Thomas G Foley, CAE
Vice President, Membership & Customer Development

Signature _____



Date _____

**XXXX SECTION IFT [PROCESSOR]**
[NAME]
Section President/Chair

Signature _____
Date _____

**EXHIBIT 1**

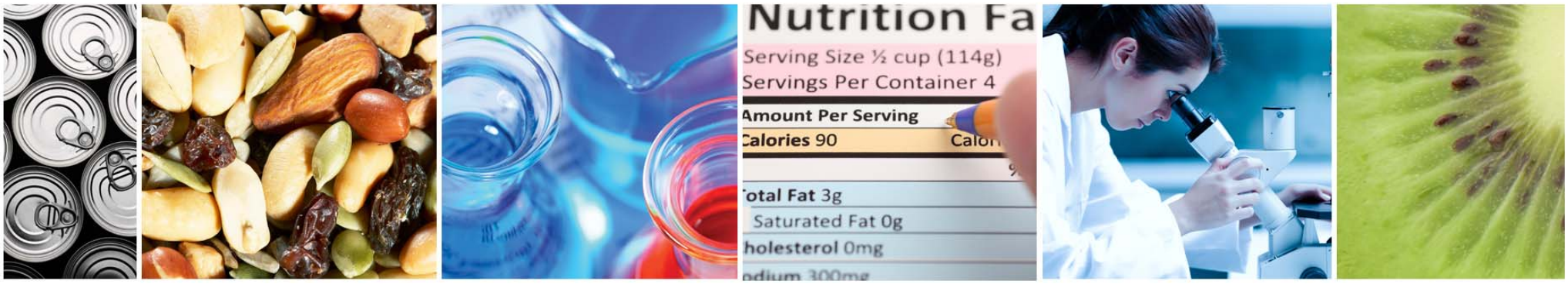
List of Personal Data types to be processed

i. IFT regularly provide sections leaders with access to rosters of section member and contact information including membership and demographic information.

**EXHIBIT 2**

List of Subcontractors

i. [TO BE COMPLETED BY SECTION]




# Section Vendor DPAs

# IFT's Experience Implementing Vendor DPAs

- We have implemented 14 of the appr. 30 vendor DPAs that we need, and 2 others are in progress
- Of these, many are based on a standard DPA template that our legal counsel developed for us
- Technology vendors often have their own standard DPA
- In every situation but one, IFT is the Controller in vendor DPAs we have completed or are pursuing
- We have seen a variety of responses from vendors when we started the DPA process with them

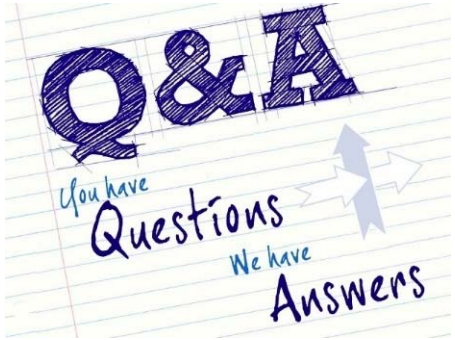
# Why Vendor DPAs Are Useful for IFT & for Sections

- DPAs reduce the likelihood of a “we didn’t agree to that” response if we ever need compliance help from a vendor
- DPAs make clear which data are being processed by a vendor, what sort of processing is being done, and why
- DPAs set clear expectations of what must happen if the vendor experiences a data breach
- DPAs identify any subprocessors that the vendor might involve with the processing
- DPAs would help demonstrate seriousness to EU regulators if we were ever audited or in receipt of a complaint

# Additional Thoughts on Section-Vendor DPAs

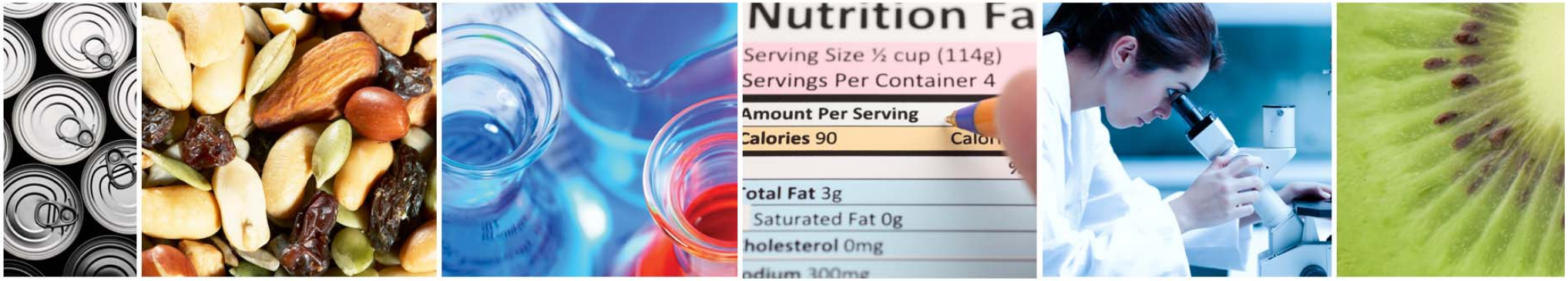
- Generally speaking, it's probably better to use a vendor-provided DPA form than to draft one that you would ask vendors to sign
- It's unlikely that you will have much negotiating leverage to modify large vendors' terms and conditions
- IFT's legal counsel is preparing guidelines for what Sections should look for in DPAs with their vendors

# QUESTIONS




**We're Here to Help!**

Email: Sections@IFT.org




# Institute of Food Technologists

**Headquarters**
525 W. Van Buren Street
Suite 1000
Chicago, IL 60607
+1.312.782.8424
ift.org

**Washington, D.C. Office**
818 Connecticut Avenue, NW
Suite 850
Washington, D.C. 20006
+1.202.466.5980
ift.org

**Tom Foley**
*VP, Membership & Customer Development*
*Email:* tfoley@ift.org
*Phone:* 312.604.0228

**Mike McCarthy**
*Director, Section Support*
*Email:* mmccarthy@ift.org
*Phone:* 312.604.0229

**Susan Andronowitz**
*Coordinator, Membership Development & Section Administration*
*Email:* sandronowitz@ift.org
*Phone:* 312.604.0238