SESSION ID: GRC-T08

GET COOKIN’ WITH GDPR—PRACTICAL TECHNIQUES AND RECIPES FOR SUCCESS

Cindy E. Compert, CIPT/M

CTO US Public Sector Market, CTO Data Security & Privacy
IBM Security
@CCBigData
Disclaimer

**Notice:** Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

- IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

None of the statements contained herein constitutes legal advice – it is process advice only.

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey here.
On the menu today...

- **Beverage**: GDPR myths and realities
- **Appetizer**: Have a good map
- **Main course**: Know your risks and vulnerabilities
- **Side dish**: Track data subject rights, audit trails
- **Dessert**: Incident Response
- **Recommendations** (and bonus recipe!)
Recipe #1 Beverage!

Mama’s Mai Tai- Mama’s Fish House, Maui

Ingredients

- 1 1/2 ounces light Rum
- 1 1/2 ounces pineapple juice
- 1 1/2 ounces lime juice
- 1 splash orgeat (almond flavored syrup)
- 1 splash simple syrup
- 2 splash orange curacao
- 2 splash grenadine or Pomegranate syrup.
- 2 ounces dark Rum float on top

Steps

1. Pour light Rum on ice in glass.
2. Add juices & orgeat sugar syrup & 1/2 of the curacao, grenadine
3. Float dark Rum and give it one quick stir.
4. Rest or the orange curacao & grenadine splashes.
5. Garnish with a lime wheel, umbrella & cherry, and tropical flower. Close your eyes and enjoy a tropical interlude 😊

- For non-alcoholic version, omit rum and curacao and double pineapple juice + orgeat. Or be lazy and use POG (Pineapple-Orange-Guava Juice)

IBM’s overall GDPR framework: Five phases to readiness

<table>
<thead>
<tr>
<th>Phase</th>
<th>Assess</th>
<th>Design</th>
<th>Transform</th>
<th>Operate</th>
<th>Conform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Conduct GDPR risk and privacy assessments across governance, people,</td>
<td>• Design governance training, communication and processes standards</td>
<td>• Develop and embed procedures, processes, and tools</td>
<td>• Execute all relevant business processes</td>
<td>• Monitor, assess, audit, report and evaluate adherence to GDPR standards</td>
</tr>
<tr>
<td></td>
<td>processes, data, security</td>
<td>• Design privacy, data management and security management standards</td>
<td>• Deliver GDPR training</td>
<td>• Monitor security and privacy using TOMs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Develop GDPR Readiness Roadmap</td>
<td></td>
<td>• Develop and embed standards using Privacy by Design, Security by Design</td>
<td>• Manage consent and data subject access rights</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identify and map personal data</td>
<td></td>
<td>• Detailed Data Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outcome</td>
<td>Assessments and roadmap</td>
<td>Defined implementation plan</td>
<td>Process enhancements completed</td>
<td>Operational framework in place</td>
<td>Ongoing monitoring and reporting</td>
</tr>
<tr>
<td></td>
<td>Identify GDPR impact and plan Technical and Organisational Measures (TOMs)</td>
<td>Includes Data Protection controls, processes and solutions to be implemented.</td>
<td>TOMs in place: Personal Data discovery, classification and governance in place</td>
<td>Begin the new GDPR ready way of working</td>
<td>Monitor TOMs execution; deliver compliance evidence to internal and external stakeholders</td>
</tr>
</tbody>
</table>
What companies should be doing as they prepare (1 of 2)

<table>
<thead>
<tr>
<th>Understand the obligations</th>
<th>Create a cross-functional GDPR team</th>
<th>Appoint a Data Protection Officer</th>
<th>Know what data is stored and where it is located</th>
</tr>
</thead>
<tbody>
<tr>
<td>Become familiar with the proposed GDPR requirements and monitor the development of implementation guidance.</td>
<td>Ensure that all aspects of the business that are impacted are part of the development and implementation of any changes.</td>
<td>Create a structured privacy office &amp; appoint, if required, a data protection officer (DPO) who has expert knowledge on data protection law.</td>
<td>Conduct a data inventory and mapping initiative to assist in understanding and evaluating the operational and technological changes required for compliance.</td>
</tr>
</tbody>
</table>

- **Review all privacy policies and statements**: Confirm all privacy notices are presented in clear and plain language, are transparent, and are easily accessible to data subjects.

- **Review customer consent and choice mechanisms**: Ensure that the appropriate consent and choice mechanisms are in place and/or are updated to meet the new consent requirements and to easily facilitate customer choice.

- **Review processes addressing data subjects’ access, correction and erasure requests**: Confirm that the operational and technical measures are in place to support these requests.

- **Review data retention schedules**: Confirm data is only held for as long as there is a legitimate business need or as may otherwise required by law.
Limited on time or resources? These are good starting point activities.
There is a class of organizations who are better prepared for GDPR and see it, not just as a compliance challenge, but a transformational opportunity.

They are taking a customer-centric approach to their efforts and exhibit thoughtfulness in building trust with their data subjects.

They are also using their preparation as an opportunity to advance their digital reinvention and drive value for their entire organization.
Respondents are seeing the potential upside of GDPR

Overall view of GDPR

- A chance to transform our privacy, security, and data management efforts: 39%
- A mandatory regulation to be complied with: 36%
- A catalyst to create new data-led business models: 20%
- An impediment to innovation and data-led business models: 5%

Source: 2018 IBM Institute for Business Value Study
Areas of focus for organizations are also areas of struggle

<table>
<thead>
<tr>
<th>#1 focus area</th>
<th>#1 struggle</th>
<th>GDPR component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Performing data discovery and ensuring data accuracy</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Complying with data processing principles</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>Developing/updating privacy policies and notices</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>Establishing a Data Protection Officer (DPO)</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>Getting consent from data subjects</td>
</tr>
</tbody>
</table>

Note: Respondents were asked to rank their top three focus areas and struggles from a list of 11 different GDPR preparation components.

Source: 2018 IBM Institute for Business Value Study
Tip 1: Have a good map
Establish a repeatable process for protecting data

**Critical Data Protection Program**

**Define**
- What personal data?
  - Understand overall data security strategy
  - Determine data protection objectives
  - Develop organizational data model / taxonomy
- Where is it? How is it used?
  - Understand data environment, infrastructure and lifecycle
  - Perform iterative discovery, analysis and classification
- What is required to protect critical data?
  - Establish baseline security requirements for personal data
  - Assess current data security processes and controls
  - Determine gaps and identify solutions

**Discover**
- How to plan, design and implement?
  - Plan and prioritize technical and business process transformations
  - Design and implement solutions that protect critical data, enable access and align to business growth objectives

**Baseline**
- How to manage critical data protection?
  - Develop governance framework, risk metrics and monitoring processes
  - Periodically validate data protection strategy and methodology
Tip 2: Data- People- Applications: Where are your risks?
Tip 3: Track data subject’s right to access, modify, delete, transfer data
Tip 4: Track where data is processed
Tip 5: You need to support 72-hour breach notification

Incident Response Platform

REQUIREMENTS

- Integrate other security technologies into a single hub
- Workflow configuration and process automation
- Empower teams to analyze, respond, resolve and mitigate incidents faster

- GDPR Preparatory Guide
  - Preparatory checklist
- GDPR Simulator
  - Breach notification timelines and regulations available inside task instructions
- GDPR-Enhanced Privacy Module
  - Seamless transition for responders and privacy professionals, task lists help with compliance
Demonstration
Recommendations
Apply What You’ve Learned..
Conduct a Readiness Assessment

Next week: Conduct a gap analysis if you have not already done so. Identify impacted business areas. Evaluate current practices against the new requirements – focus on process development, best practices and organizational need. Appoint GDPR ‘Czars’ in business units to coordinate activities.

30 days: Have a basic data map completed, listing major applications that handle personal data; prioritize customer-facing and high risk applications. Define a **maturity model and gap/remediation plan** to help develop and implement your compliance roadmap.

60 days-90 days and beyond: Continue working gap analysis, focus on repeatable processes and demonstrating conformance.

---

This should not be considered Legal advice – it is process advice only.

Reach out to the appropriate Legal Counsel for guidance.
THANK YOU

Cindy Compert
CTO US Public Sector Market, CTO Data Security & Privacy
@CCBigData
Helpful Links

- IBM’s GDPR Readiness, Data Responsibility: [www.ibm.com/gdpr](http://www.ibm.com/gdpr)
### IBM Security GDPR framework: Key activities to address GDPR

<table>
<thead>
<tr>
<th>Privacy requirements</th>
<th>Security requirements</th>
<th>Assess</th>
<th>Design</th>
<th>Transform</th>
<th>Operate</th>
<th>Conform</th>
</tr>
</thead>
</table>
| PREPARE:  
- Conduct GDPR assessments, assess and document GDPR-related policies  
- Assess data subject rights to consent, access, correct, delete, and transfer personal data  
- Identify access risks, supporting Privacy by Design | PREPARE:  
- Assess security current state, identify gaps, benchmark maturity, establish conformance roadmaps  
- Identify vulnerabilities, supporting Security by Design  
- Discover and classify personal data assets and affected systems | ROADMAP:  
- Create GDPR remediation and implementation plan  
PRIVACY BY DESIGN:  
- Design policies, business processes and supporting technologies  
- Create GDPR reference architecture  
- Evaluate controller or processor governance | TRANSFORM PROCESSES:  
- Implement and execute policies, processes and technologies  
- Automate data subject access requests | MANAGE GDPR PROGRAM:  
- Manage GDPR data governance practices such as information lifecycle governance  
- Manage GDPR enterprise conformance programs such as data use, consent activities, data subject requests | DEMONSTRATE:  
- Record personal data access audit trail including data subject rights to access, modify, delete, transfer data  
- Run data processor or controller governance including providing processor guidance, track data processing activities, provide audit trail, preparing for data subject access requests | RESPOND:  
- Respond to and manage breaches |
| DISCOVER:  
- Discover and classify personal data assets and affected systems  
- Identify access risks, supporting Privacy by Design | RUN SERVICES:  
- Monitor personal data access  
- Govern roles and identities  
- Develop GDPR metrics and reporting schemas | | | | | |
| SECURITY BY DESIGN:  
- Create security reference architecture  
- Design Technical and Organizational Measures (TCMs) appropriate to risk (such as encryption, tokenization, dynamic masking)  
- Implement security controls; mitigate access risks and security vulnerabilities | MANAGE SECURITY PROGRAM:  
- Manage and implement security program practices such as risk assessment, roles and responsibilities, program effectiveness  
- Monitor security operations and intelligence: monitor, detect, respond to and mitigate threats  
- Govern data incident response and forensics practices | | | DEMONSTRATE:  
- Demonstrate technical and organizational measures to ensure security appropriate to processing risk  
- Document security program: ongoing monitoring, assessment, evaluation and reporting of security controls and activities |
| PROTECT:  
- Implement privacy-enhancing controls (for example, encryption, tokenization, dynamic masking) | | | | | RESPOND:  
- Respond to and manage breaches |
## Article 30 Records of Processing

**UK ICO example:** (sample templates available for download);

Summary:

1. Identify and classify personal data, centralize definitions
2. Identify/mitigate data risks
3. Identify/mitigate application risks
4. Identify/mitigate people risks especially with back end data sources
5. Create audit trails and reporting for data subject rights in databases
6. Create audit trails, block inappropriate access for files
7. Use Robotic Process Automation (RPA) to automate data subject access requests
Demonstration: Automation makes discovery and classification faster and more efficient

- Using scanning and AI to locate, identify and classify personal data
- This short demonstration shows how scanning techniques such as metadata searching, pattern matching, and AI can be used to locate personal data, classify it into monitoring groups, and prepare to monitor data access.
Demonstration: Identity Governance

- Using Identity Governance to find and mitigate personal data access risks at the ‘people’ layer
- This demonstration shows how data protection and identity governance can be combined to identify and mitigate access risks from database access entitlements, an often overlooked area.
Demonstration: Data Risk Dashboard

- Using a risk dashboard to find and mitigate personal data access risks at the data layer
- This demonstration shows how to link business processes and business areas to underlying personal data assets in order to surface, prioritize, and mitigate data layer risks.
Demonstration: Audit Trails and Data Subject Rights

- Demonstrate data access and data subject rights audit trails
- Demonstrate Robotic Process Automation (RPA) to help automate Data Subject Rights by leveraging existing business processes and applications
Robotic Process Automation Demo Flow

1. ABC Company customer sends the data access request to abc.gdpr@gmail.com from their registered email id with their customer id in the subject line.

2. ABC Company has automated this task using IBM RPA
   1. Bot reads email of customer
   2. Extracts customer id from mail
   3. Uses customer id to query Excel sheet in which customer master data is maintained
   4. Get Personal data of customer like Name, Date of Birth, Address etc
   5. Use this data to query Box repository for documents (Company tags documents by name+dob of customers)
   6. Download documents found on Box
   7. Attaches documents as well as personal data in a mail
   8. Respond back to customer.

3. The BOT runs 24 by 7, and can either directly respond to customer mail or it can be send to Company legal resource, who verify mail and send it to customer.
How do I find and manage my data risks?

**Data Risk Dashboard**

- Identify high-value, business-sensitive information assets that are at risk from internal and external threats.
- Gain visibility into data processors and data controllers, for both applications and business processes.
- Visualize data exposure to help executives have conversations with IT, security and the line of business.

![Image of IBM Data Risk Manager Dashboard]

- Map data residency and vulnerabilities
- Visualize sensitive data information
- How do I find and manage my data risks?
- Top information assets at risk
- Vulnerabilities histogram

**Geographic Distribution of Information Assets**

**Organizational Distribution of Crown Jewels Data**

**Information Asset Policy Violations and Vulnerabilities**

**Quarterly Vulnerability Trends**
Who has access to my data, and is there a risk?

**Identity Governance**

- Quickly onboard, manage and simplify identity management
- Identify risk and highlight segregation of duties violations across enterprise and cloud applications
- Employ algorithms for role mining, modeling, optimization and analytics to lower risk
- Provide end-to-end user lifecycle management

Identify and mitigate access risks and automate user and identity lifecycle processes
How do I know where my application risks are?

Application Vulnerability Scanning

- Identify vulnerabilities assessed against articles 25 and 32.
- Allows organizations to implement fixes and help reduce security risks.

Body Parameters Accepted in Query

| Risk: | It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations. |
| Causes: | Insecure web application programming or configuration |
| Fix: | Do not accept body parameters that are sent in the query string |

<table>
<thead>
<tr>
<th>Severity</th>
<th>URL</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td><a href="http://pghealth.com:8080/PrettyGoodIntake/PatientSearch">http://pghealth.com:8080/PrettyGoodIntake/PatientSearch</a></td>
<td></td>
</tr>
</tbody>
</table>

Email Address Pattern Found

| Risk: | It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations. |
| Causes: | Insecure web application programming or configuration |
| Fix: | Remove e-mail addresses from the website |

<table>
<thead>
<tr>
<th>Severity</th>
<th>URL</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td><a href="http://pghealth.com:8080/PrettyGoodIntake/PatientSearch">http://pghealth.com:8080/PrettyGoodIntake/PatientSearch</a></td>
<td>PatientSearch</td>
</tr>
</tbody>
</table>

Article 32(1)(a) - Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data.
Data Classification and Audit Trails

- Data discovery and classification for personal data
- Auditing and monitoring reports for GDPR personal data including data subject requests and personal data access
- Compliance workflows for notifications to auditors, controllers and the Data Privacy Officer

Tip 4: Track where data is processed including data subject rights
Robotic Process Automation helps with automated handling of data subject access requests

Using RPA, one can automate email processing, extraction of customer name, search on legacy system, attaching KYC documents and responding to mail.

- RPA bot gathers & correlates data from backend systems
- Interacts with MDM/Excel system to create response mail with attachments

Back IT systems – Emails, Box, ECM, Excel, SAP, Mainframe, CRM, bespoke applications, MDM

- Replaces 25 manual activities

Robotic Process Automation:
- Interacts directly with web & desktop application screens
- Does not require that apps have APIs
1. ABC Company customer sends the data access request to abc.gdpr@gmail.com from their registered email id with their customer id in the subject line.

2. ABC Company has automated this task using IBM RPA
   1. Bot reads email of customer
   2. Extracts customer id from mail
   3. Uses customer id to query Excel sheet in which customer master data is maintained
   4. Get Personal data of customer like Name, Date of Birth, Address etc
   5. Use this data to query Box repository for documents (Company tags documents by name+dob of customers)
   6. Download documents found on Box
   7. Attaches documents as well as personal data in a mail
   8. Respond back to customer.

3. The BOT runs 24 by 7, and can either directly respond to customer mail or it can be send to Company legal resource, who verify mail and send it to customer.
Tip 5: You need to support breach management and notification including incident forensics

What is it?
GDPR Article 33, “In the case of a personal data breach, the controller shall without undue delay and, where feasible, *not later than 72 hours* after having become aware of it, notify the personal data breach to the supervisory authority. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.”

Why it matters:
Both processors and controllers have responsibilities to report breaches in a timely manner, or risk substantial fines. EU has never had mandated breach reporting. Organizations will struggle with coordinating the people, process, and information needed to report and respond to a breach within the 72 hour window.
Automate your Incident Response

GDPR Privacy Violation - QRadar Source IP - 192.168.42.193, ID: 187

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>2099</td>
</tr>
<tr>
<td>Phase</td>
<td>Engage</td>
</tr>
<tr>
<td>Severity</td>
<td>—</td>
</tr>
<tr>
<td>Date Created</td>
<td>09/10/2016</td>
</tr>
<tr>
<td>Date Occurred</td>
<td>09/07/2016</td>
</tr>
<tr>
<td>Date Discovered</td>
<td>09/07/2016</td>
</tr>
<tr>
<td>Data Compromised</td>
<td>Yes</td>
</tr>
<tr>
<td>Incident Type</td>
<td>Phishing, System Intrusion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR Privacy Violation - 1 events in 1 categories: SQL Injection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Document the incident</td>
<td>Andy Scott 03/19/2018</td>
</tr>
<tr>
<td>* Alert the data protection officer</td>
<td>Andy Scott 03/20/2018</td>
</tr>
<tr>
<td>* Verify risk of harm</td>
<td>DPO User 03/20/2018</td>
</tr>
<tr>
<td>* Document the category of lawful data processing</td>
<td>Jack Jones 03/20/2018</td>
</tr>
<tr>
<td>* Reexamine risk mitigation/compliance processes, procedures, and documentation</td>
<td>Kevin Manley 03/21/2018</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Determine if a cross-border data transfer agreement is applicable</td>
<td>Attty Lawyer 03/22/2018</td>
</tr>
<tr>
<td>* Notify const update</td>
<td></td>
</tr>
<tr>
<td>* Notify exten appropriate</td>
<td></td>
</tr>
<tr>
<td>* Take steps or execution attacks</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Notify Affected Individuals (France)</td>
<td>DPO User 03/30/2018</td>
</tr>
<tr>
<td>* HIPAA Other Notifications</td>
<td>Unassigned 04/06/2018</td>
</tr>
<tr>
<td>* Notice to CA Media</td>
<td>Unassigned</td>
</tr>
</tbody>
</table>

Tasks Were Updated

The following 11 tasks were added:
- Alert the data protection officer
- Determine if a cross-border data transfer agreement is applicable
- Determine supervisory authority(ies)
- Document the category of lawful data processing
- Document the incident
- Evaluate privacy and data protection policies and processes
- If determined to be necessary, notify the data subject(s) of the breach
- Notify the supervisory authority(ies) of the breach
- Reexamine risk mitigation/compliance processes, procedures, and documentation
RECIPIES
Sharon Ames’ Quickie Hummus

- 1 16 oz. can of chickpeas
- 1/4 cup tahini (Middle Eastern paste made of ground sesame, available in specialty grocery stores, frequently at regular stores)
- 1-2 tablespoons fresh lemon juice
- 1-2 garlic cloves (optional)

Blend ingredients and add salt to taste. Serve with pita bread and raw veggies (carrots, celery, jicama, broccoli, snap peas, etc.)

Sharon says there is no excuse not to make fresh hummus, it’s so easy!
Crazy Easy Oven Baked Ribs

- 1 rack baby back ribs
- Adobo seasoning - available in Latin foods section or make your own - I use O Organics brand from Safeway
- Your favorite BBQ sauce. I use Bullseye or Stubbs Original

Heat oven to 300 degrees F.

Rub Adobo all over ribs - 1-2 tablespoons should be more than enough.

Bake for 2-2 1/2 hours until dark brown and fat is rendered out (see example).

Brush on BB sauce and cook another 30 minutes

Serve and enjoy!
**Asian Cucumber Salad**

- 2 English cucumbers, sliced or cubed
- 1/3 cup rice wine vinegar
- 1/4 cup minced sweet onion
- 1 teaspoon low sodium soy sauce
- 1/2 teaspoon Thai sweet chili sauce or brown sugar
- 2 teaspoons toasted sesame oil
- 1/8 teaspoon freshly grated ginger
- 1 Tablespoon toasted sesame seeds for garnish

Place cucumbers in serving bowl. Combine remaining ingredients except for sesame seeds in a separate bowl, whisk to combine. Pour over cucumbers and top with sesame seeds. Tastes better if you refrigerate for an hour or more. Optional: add 1 C cubed firm tofu or garbanzo beans.

Adapted from https://www.twopeasandtheirpod.com/asian-cucumber-salad/
Mom’s Baked Apples

- 4 BAKING apples—Braeburn are really nice and hold shape
- 1/2 cup Raisins
- 1/2 teaspoon cinnamon
- 1-2 tablespoons sugar (to taste)
- 1 T Butter
- Port Wine
- Vanilla Ice Cream (optional)

Preheat oven to 350

Cut off tops and core apples but leave bottom closed

Mix 1/4c raisins, cinnamon, and sugar in bowl, stuff insides, put extra in bottom of baking dish w/apples. Add water about 1/2 inch or more-you can use apple juice or even add some port! Sprinkle a little cinnamon-sugar mix on inside of apple (outside core area). Dot w/butter.

Bake for about an hour.

Be sure to serve with vanilla ice cream; pour port wine over top for extra flavor (Mom did not use Port but I think it’s a nice touch)
Bonus Recipe! BAKED Coconut shrimp with apricot dipping sauce (15 min prep., 15 min cook time)

- 1 pound large shrimp, peeled and deveined. Leave tails on
- 1/3 cup cornstarch
- 1/4 teaspoon salt
- 1/4 teaspoon cayenne pepper to taste
- 1 cups flaked sweetened coconut /1 c panko breadcrumbs combined
- 2 eggs beaten (egg whites if you want to go lower cal).

Steps
- Preheat oven to 400 degrees F (200 degrees C) line baking sheet with foil, spray lightly with cooking spray
- Rinse and dry shrimp with paper towels. Line up 3 bowls. Bowl 1: Mix cornstarch, salt, and cayenne pepper; Bowl 2: eggs; Bowl 3: coconut flakes and panko. For each shrimp, dredge in cornstarch mixture, dip in egg (shake off excess), and roll in the coconut/panko. Place on the baking sheet.
- Bake shrimp until bright pink on outside, opaque in center, and breading is lightly browned, 15 to 20 minutes, flipping the shrimp halfway through.

Apricot Dipping Sauce
- 1/2 cup apricot jam
- 1 tsp. freshly grated ginger
- 1 tsp. Dijon mustard- use Chinese if you have it
- 2 T freshly squeezed lime juice or Key Lime Juice

Add a little salt for zing
Mix and enjoy!