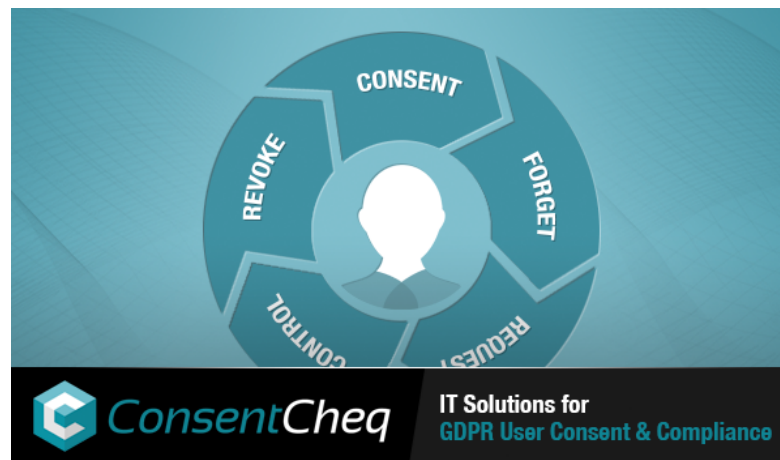




PrivacyCheq



GDPR Triage

Featuring guest speaker
Constantine Karbaliotis of Nymity

NYMITY

THIS PRESENTATION AND THE INFORMATION IN IT ARE PROVIDED IN CONFIDENCE, FOR THE SOLE PURPOSE OF PRIVACYCHEQ, AND MAY NOT BE DISCLOSED TO ANY THIRD PARTY OR USED FOR ANY OTHER PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF PRIVACYCHEQ.



Andrew Smith

Privacy Engineer

844 243 2437 x118

ahs@privacycheq.com





NYMITY

Constantine
Karbaliotis

CIPP/US/C/E, CIPM, CIPT, FIP
Vice President of Privacy Office Solutions
– NYMITY
and former CPO





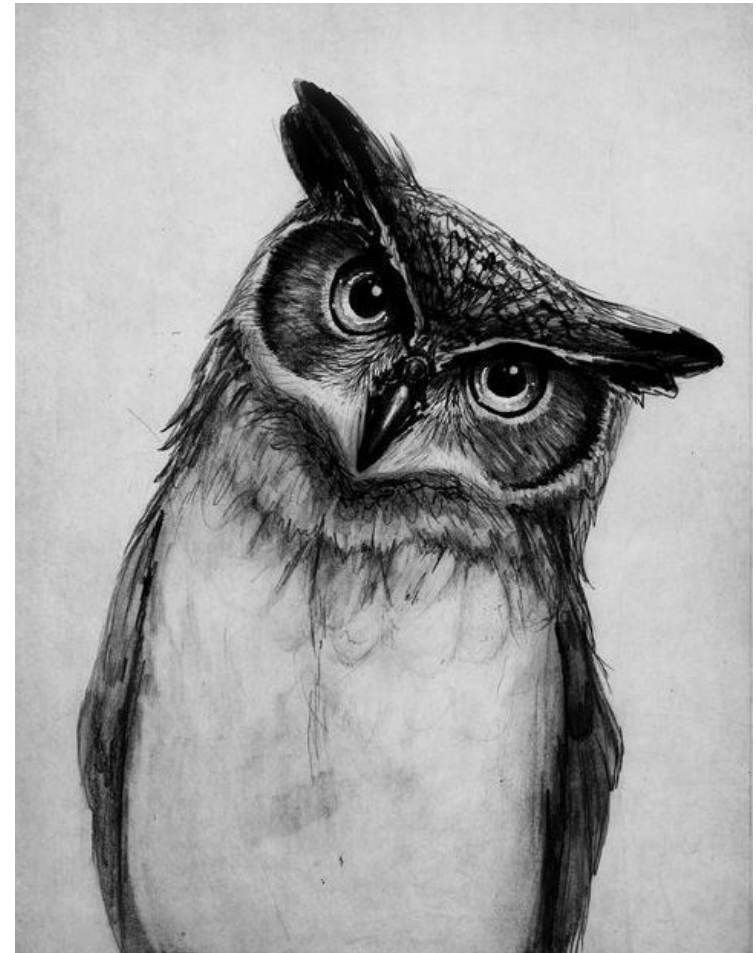
Email Us

Andrew

ahs@privacycheq.com

Constantine

constantine.karbaliotis@nymity.com



Agenda



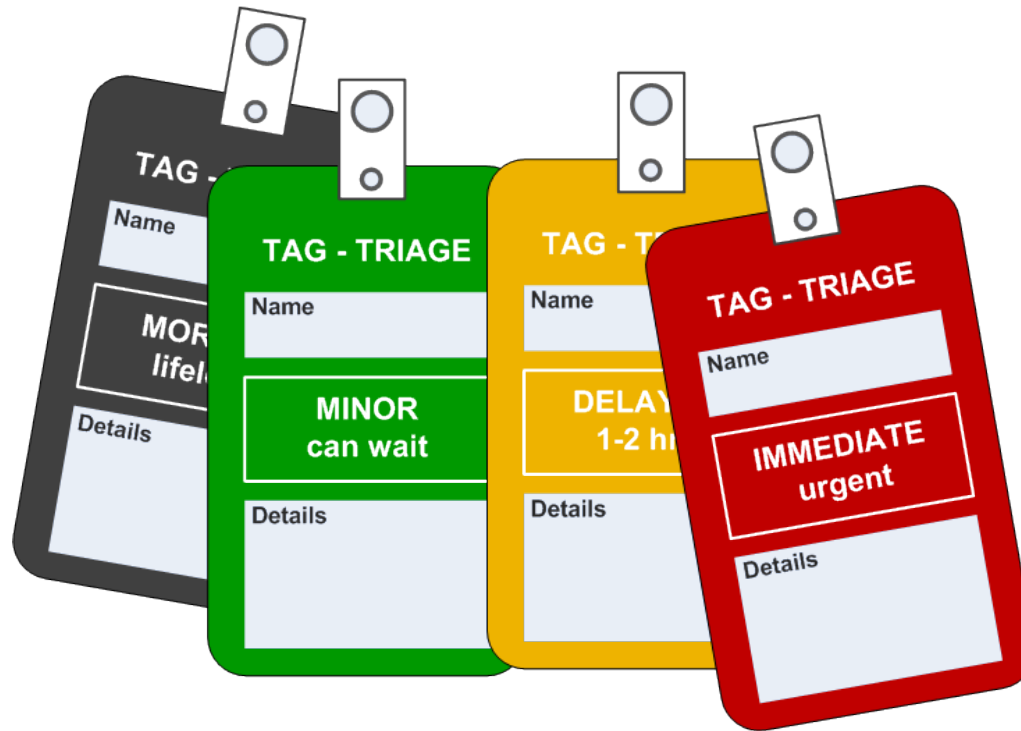
- What is Triage
- What are the reasons for Triage in the context of GDPR
- Describe a comprehensive privacy program
- Contrast with a Triage approach

What is Triage



M * A * S * H

What is Triage



“assigning of priority order to projects on the basis of where funds and other resources can be best used, are most needed, or are most likely to achieve success”

Reasons for Triage



- Limited Time



Reasons for Triage



- Limited Time
- Limited Budget



Reasons for Triage



- Limited Time
- Limited Budget
- Supervisory Authorities' Limited Attention



Reasons for Triage



- Limited Time
- Limited Budget
- Supervisory Authorities' Limited Attention
- So Many Other Well-Deserving Targets

IN CASE OF ZOMBIE ATTACK

REMEMBER

**YOU DON'T NEED
TO OUTFRAN THE
ZOMBIE**

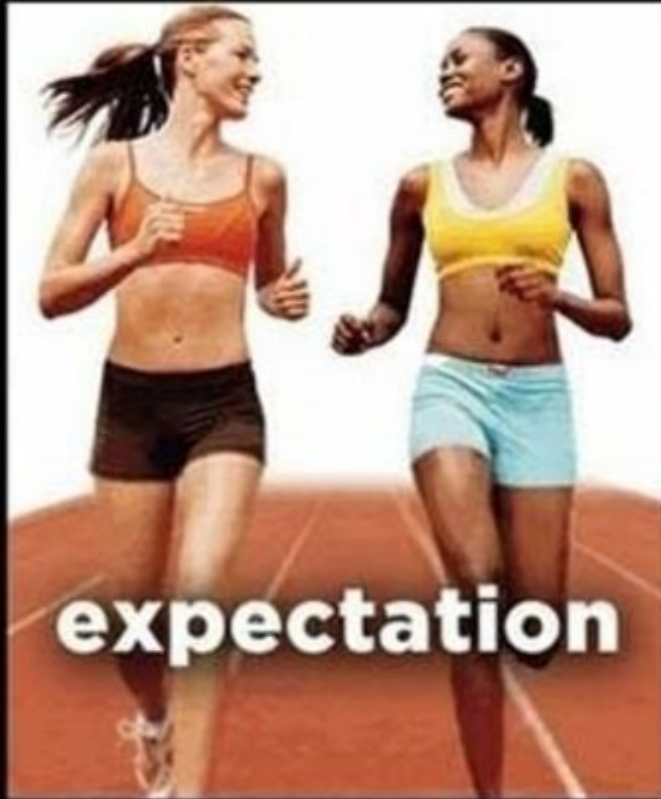


**YOU JUST NEED
TO OUTFRAN
YOUR FRIENDS**

Expectation vs. Reality



NEW YEARS RESOLUTION



The difference between treatment and triage



A comprehensive privacy program

What you want to address in the fullness of time...

- Maintain Governance Structure
- Maintain a personal data inventory and data transfer mechanisms
- Maintain internal data privacy policy
- Embed data privacy into operations
- Maintain training and awareness program
- Manage Information Security Risk
- Manage Third-party risk
- Maintain Notices
- Respond to requests and complaints from individuals
- Monitor for new operational practices
- Maintain data privacy breach management program
- Monitor data handling practices
- Track external criteria

Triage

What you are left doing in the time you have available...

- Understand where your data is and how it is moving
- Ensure your privacy policy reflects what you are doing with personal data
- Be able to honour what you commit to
Ensure you can respond to subject access requests – what do you know about an individual
- Be able to respond promptly to issues and complaints, and de-escalate at the lowest level possible
- Be able to respond to inquiries about the state of your privacy program – what is your story?
- Empower customers to make privacy choices

Nymity Privacy Management Accountability Framework



UPDATED MARCH 2017

Nymity Privacy Management Accountability Framework™

A Menu of Privacy Management Activities (Technical and Organizational Measures)

NYMITY
innovating compliance



1. Maintain Governance Structure

Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

Privacy Management Activities

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, Privacy Counsel, CPO, Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer/Official (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Report to external stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to internal stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment
- Integrate data privacy into business risk assessments/reporting
- Maintain a Privacy Strategy
- Integrate a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies



2. Maintain Personal Data Inventory and Data Transfer Mechanisms

Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

Privacy Management Activities

- Maintain an inventory of personal data holdings (what personal data is held and where)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain flow charts for data flows (e.g. between systems, between processes, between countries)
- Maintain records of the transfer mechanism used for cross-border data flows (e.g. standard contractual clauses, binding corporate rules, approvals from regulators)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use the EU-US Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism



3. Maintain Internal Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

Privacy Management Activities

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)



4. Embed Data Privacy Into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into email marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and/or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)



5. Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

Privacy Management Activities

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training, such as HR, security, call centre
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/event)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain certification for individuals responsible for data privacy, including continuing professional education



6. Manage Information Security Risk

Maintain an information security program based on legal requirements and ongoing risk assessments

Privacy Management Activities

- Integrate data privacy risk into security risk assessments
- Integrate data privacy into an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewall, monitoring)
- Use the EU-US Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture
- Maintain a security certification (e.g. ISO)



7. Manage Third-Party Risk

Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors
- Review long-term contracts for new or evolving data privacy risks



8. Maintain Notices

Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain a data privacy notice that details the organization's personal data handling practices
- Provide data privacy notices at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. email, flyers, offers)
- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust



9. Respond to Requests and Complaints from Individuals

Maintain effective procedures for interactions with individuals about their personal data

Privacy Management Activities

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests for access to or reuse of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Monitor and report metrics for data privacy complaints (e.g. number, root cause)



10. Monitor for New Operational Practices

Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

Privacy Management Activities

- Integrate Privacy by Design into system and product development
- Maintain PIA/DPIAs guidelines and templates
- Conduct PIA/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIA/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)



11. Maintain Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

Privacy Management Activities

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage



12. Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

Privacy Management Activities

- Conduct self-assessments of privacy management
- Conduct Internal Audit of the privacy program (i.e. operational audit of the Privacy Office)
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators



13. Track External Criteria

Track new compliance requirements, expectations, and best practices

Privacy Management Activities

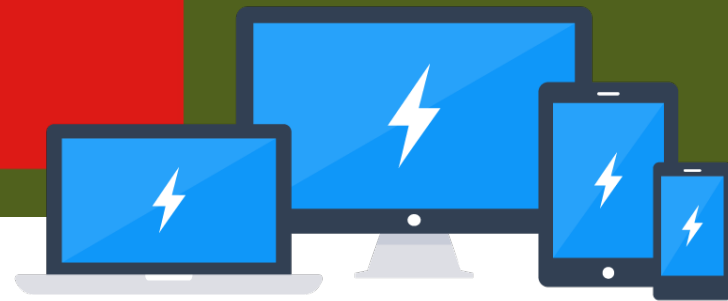
- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting services/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

The Nymity Privacy Management Accountability Framework™ was developed based on Nymity's global research on data privacy accountability. The Framework is a comprehensive listing of over 130 Privacy Management Activities (PMAs) categorized into 13 Privacy Management Categories (PMCs). Once implemented, the activities highlighted in BLUE will help achieve ongoing compliance with the GDPR and produce documentation to demonstrate compliance.

Copyright © 2017 by Nymity Inc. All rights reserved. All text, images, logos, trademarks and information contained in this document are the intellectual property of Nymity Inc. unless otherwise indicated. Reproduction, modification, transmission, use, or quotation of any content, including text, images, photographs etc., requires the prior written permission of Nymity Inc. Requests may be sent to info@nymity.com.



M * A * S * H



Get a handle on your data





Policy

A **policy** is described
government, private
"Statement of Inter
important organiza



Please Notice This



Create an appropriate privacy notice



Privacy Policy

INGREDIENTS: ENRICHED FLOUR (WHEAT FLOUR, NIACIN, REDUCED IRON, THIAMIN MONONITRATE [VITAMIN B₁], RIBOFLAVIN [VITAMIN B₂], FOLIC ACID), CORN SYRUP, SUGAR, SOYBEAN AND PALM OIL (WITH TBHQ FOR FRESHNESS), CORN SYRUP SOLIDS, DEXTROSE, HIGH FRUCTOSE CORN SYRUP, FRUCTOSE, GLYCERIN, CONTAINS 2% OR LESS OF COCOA (PROCESSED WITH ALKALI), POLYDEXTROSE, MODIFIED CORN STARCH, SALT, DRIED CREAM, CALCIUM CARBONATE, CORNSTARCH, LEAVENING (BAKING SODA, SODIUM ACID PYROPHOSPHATE, MONOCALCIUM PHOSPHATE, CALCIUM SULFATE), DISTILLED MONOGLYCERIDES, HYDROGENATED PALM KERNEL OIL, SODIUM STEAROYL LACTYLATE, GELATIN, COLOR ADDED, SOY LECITHIN, DATEM, NATURAL AND ARTIFICIAL FLAVOR, VANILLA EXTRACT, CARNAUBA WAX, XANTHAN GUM, VITAMIN A PALMITATE, YELLOW #5 LAKE, RED #40 LAKE, CARAMEL COLOR, NIACINAMIDE, BLUE #2 LAKE, REDUCED IRON, YELLOW #6 LAKE, PYRIDOXINE HYDROCHLORIDE (VITAMIN B₆), RIBOFLAVIN (VITAMIN B₂), THIAMIN HYDROCHLORIDE (VITAMIN B₁), CITRIC ACID, FOLIC ACID, RED #40, YELLOW #5, YELLOW #6, BLUE #2, BLUE #1.

Privacy Brief

Nutrition Facts

Serving Size 2/3 cup (55g)
Servings Per Container About 8

Amount Per Serving

Calories 230 Calories from Fat 40

% Daily Value*

Total Fat 8g **12%**

Saturated Fat 1g **5%**

Trans Fat 0g

Cholesterol 0mg **0%**

Sodium 160mg **7%**

Total Carbohydrate 37g **12%**

Dietary Fiber 4g **16%**

Sugars 1g

Protein 3g

Vitamin A 10%

Vitamin C 8%

Calcium 20%

Iron 45%

*Percent Daily Values are based on a 2,000 calorie diet.
Your daily value may be higher or lower depending on your calorie needs.

	Calories:	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g

Create an appropriate privacy notice



Be accountable for data processing



Be accountable for data processing



- Notice provided before processing
- Manage versions of the privacy notice
- Ensure consent was given by the data subject
- Document: The data subject has signed a contract with the data controller
- Notice was provided after the fact (in the case of legitimate interest)
- Control which staff may access the personal data consistently with what you have said in your notice
- Personal data is deleted or anonymized once it is no longer needed

Respond to rights requests immediately





Avoid unnecessary
scrutiny from
supervisory authorities



Respond to rights requests accurately



Data subjects have a number of rights under the law



Right to Withdraw Consent

You have the right to withdraw your consent for processing your personal data.



Right to be Informed

You have the right to be informed about what personal data is collected from you, and the purpose it will be used for.



Right of Access

You have the right to a copy of the personal data that we have collected.



Right to Rectification

You have the right to view and change inaccurate personal data that we have collected.




Right to Erasure

You have the right to be forgotten. You may ask that we erase all your personal data previously collected.

Engage with customers: enable control




Preference and Consent Management

 Consents ▾ Children ▾ Account ▾ English ▾

Consent I have given

bHive




A model to show off a layered privacy notice strategy

Consent Given: 6/16/17 11:26 AM

[REVOKE MY CONSENT](#)

[VIEW PRIVACY DIALOG](#)

ConsentCheq




The ConsentCheq Dashboard application allows users to manage their privacy and consent all in one place.

Consent Given: 6/16/17 10:28 AM

[REVOKE MY CONSENT](#)

[VIEW PRIVACY DIALOG](#)

Friendly Gesture



Friendly Gesture connects professional volunteers with needy citizens in our neighborhood


Consent Given: 6/16/17 10:31 AM

[REVOKE MY CONSENT](#)

[VIEW PRIVACY DIALOG](#)

Consent I have revoked

Grocery Max



Grocery Max's online presence gives customers the ability to think bigger about their grocery needs and give them more options about how and when to buy.

Consent Revoked: 6/16/17 10:29 AM

[CONFIRM MY CONSENT](#)

[VIEW PRIVACY DIALOG](#)

What did we learn today?



- With the time that remains before May 25, 2018, one of the key ways your organization will draw negative attention is through interactions with customers over the internet:
 - Understand where your data is and how it is moving
 - Start by developing the internal processes and policies to make sure you can do what you are committing to
 - Be able to answer questions
 - Empower customers to make privacy choices
 - Ensure you can honour their choices



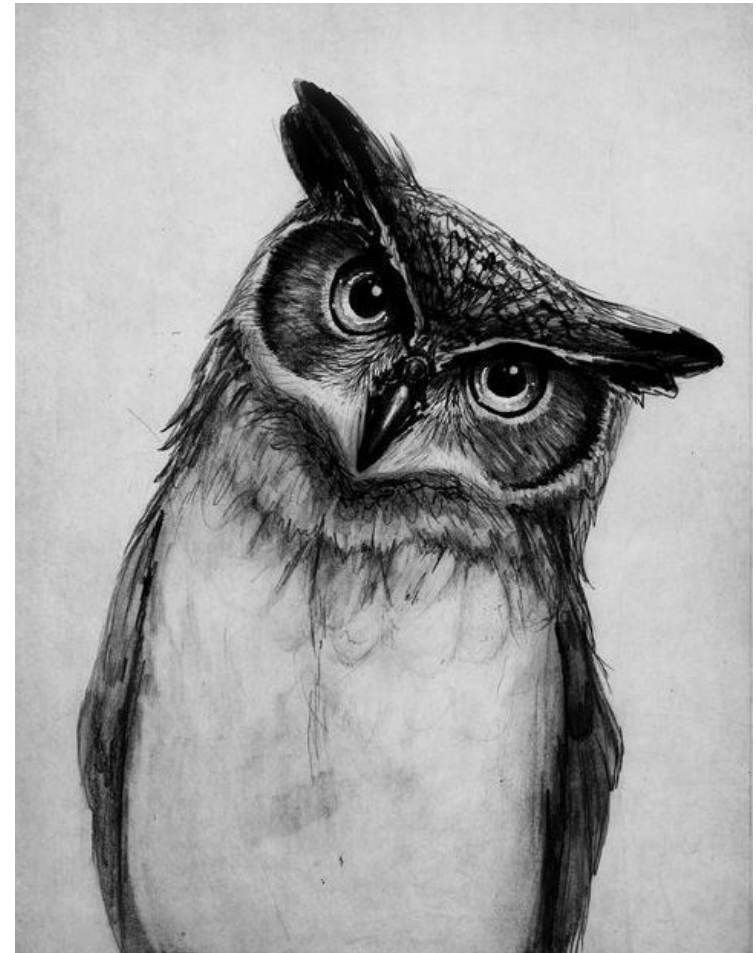
Email Us

Andrew

ahs@privacycheq.com

Constantine

constantine.karbaliotis@nymity.com





Operationalizing GDPR Webinar Series

- Consent Events Baking Show
- Operationalizing Legitimate Interest as the Basis for Lawful Processing
- ePrivacy / Cookie Technical Compliance Strategies
- Best Practices for GDPR Compliant Privacy Notices
- The GDPR Consent Lifecycle

GDPR Whitepapers

- DPO's Guide to Working with IT to Operationalize GDPR Compliance
- Technical Requirements of the GDPR

Informational Links

- The Privacy Elephant
- What "GDPR Compliance" will really mean to game publishers. It's about Privacy by Design.
- Privacy and Games - GDPR, Brexit, And Privacy Shield... Oh My!
- Privacy: How will GDPR and Privacy Shield Impact the Game Biz?
- THOUGHT LEADERS: THE FUTURE OF CONSUMER IOT

<http://www.consentcheq.com/index.php/gdpr-educational-resources/>

Coming Soon



2017 JULY						
SUN	MON	TUE	WED	THU	FRI	SAT
						1
2	3	4	5	6	7	8
9	10	11	12 NYMITY	13	14	15
16	17	18 NYMITY	19 	20	21	22
23	24	25	26	27	28	29
30	31					

Coming Soon



NYMITY

GDPR Compliance Webinar Series

Nymity has launched a webinar series: 13 Advanced GDPR Compliance Webinars. These sessions are targeted towards individuals responsible for implementing, managing and demonstrating compliance to the GDPR. Each webinar will deep dive on a specific topic relating to the GDPR, and will equip Privacy Officers with advanced knowledge, case studies, tools, and techniques to deal with complex requirements within the GDPR.

**Register at [Nymity.com](https://www.nymity.com) – Workshops and
Webinars**



PrivacyCheq



GDPR Triage

Featuring guest speaker
Constantine Karbaliotis of Nymity

NYMITY

THIS PRESENTATION AND THE INFORMATION IN IT ARE PROVIDED IN CONFIDENCE, FOR THE SOLE PURPOSE OF PRIVACYCHEQ, AND MAY NOT BE DISCLOSED TO ANY THIRD PARTY OR USED FOR ANY OTHER PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF PRIVACYCHEQ.