Öryggisflokkun gagna

Anna Kristín, Compliance Officer
and Legal Advisor

Hvaða gella er þetta?

B.Sc. Viðskiptalögfræði

ML Lögfræði

B.Sc. Viðskiptafræði með áherslu á viðskiptagreind (Business Intelligence)

HVAÐ ER ÖRYGGISFLOKKUN?

Afhverju Purview?

Gögnin okkar → Reglugerðir → Gervigreindin → Traust, ábyrgð og rekstraröryggi

Crayon

HVAÐ ER ÖRYGGISFLOKKUN?

Gervigreindin (Copilot)

- Öll gögn sem notandinn hefur aðgengi að
- Röng aðgangsstýring → óæskileg upplýsingamiðlun
- Copilot afhjúpar vandamálið → býr það ekki til
- Afhverju er þetta mikilvægt?

Gagnaöryggi og regluvarsla og verkefni tengd þeim sviðum eru ekki einungis tæknileg verkefni.

Í raun snúast þau fyrst og fremst um stefnumótandi ákvarðanir. Krefst þátttöku ólíkra sviða innan fyrirtækja og stofnanna og skýrrar forystu stjórnenda.

“No scenario exists in which IT is accountable for information assets. None.”

Sebastian Zamorano

MCT | AI-Driven Compliance Strategist | Microsoft Purview & Defender Architect | MPARR Creator | Speaker | Automating Governance at Scale

Microsoft Purview and Microsoft Defender architect with over 25 years of experience across enterprise security and compliance,

Crayon

HVAÐ ER ÖRYGGISFLOKKUN?

Öryggisflokkun gagna er „einfalt“ verkefni

Bæta merkingu/flokkun á skjal

Flokkun endurspeglast í öryggistefnunni og hegðun starfsmanna

IT ákveður ekki hvaða gögn skipta raunverulega máli fyrir fyrirtækið

Crayon

HVAÐ ER ÖRYGGISFLOKKUN?

Áskorunin á bak við öryggisflokkunina

- Fyrirtæki og stofnanir byrja frá mismunandi stöðum
  - Oft hjá upplýsingatækni
  - Stjórnendum
  - Regluvörslu
- Árangurinn ræðst af **Skýrleika, samvinnu** og **samþættingu**
- Ein stærsta áskorunin er að gera flokkunina **skiljanlega** og **merkingarbæra** fyrir starfsfólk

Öryggisflokkun gagna íslenska ríkisins

Opin gögn

Ópersónugreinanleg gögn eða gögn sem eru opin og aðgengileg til notkunar og endurnotkunar. Svo gögn teljist opin þurfa þau að vera tiltæk án umsókna / beiðna og vera aðgengileg óháð tíma.

Varin gögn

Öll gögn önnur en opin gögn sem eru hluti af daglegum rekstri ríkisaðila. Varin gögn geta þó verið misviðkvæm og krafist sérsniðinna öryggisúrræða í samræmi við niðurstöður áhættumats. Gögn sem verja skal bæði vegna hagsmuna einstaklinga (Persónuvernd) og lögaðila.

Sérvarin gögn

Gögn sem vegna viðkvæmrar stöðu m.t.t. tímasetninga eða innihalds geta valdið víðtæku og langvarandi tjóni fyrir hópa einstaklinga, lögaðila eða ríkisaðila.

Afmörkuð gögn

Gögn sem eru viðkvæm fyrir samfélagið í heild eða stöðu þjóðarinnar á alþjóðavettvangi

Crayon

Íslenski markaðurinn

Opin gögn

Fyrir efni sem er ætlað til opinberrar eða ytri dreifingar.
Felur ekki í sér áhættu sé deilt utan fyrirtækisins eða stofnunarinnar.
Engin dulkóðun

Innri gögn

Gögn sem eiga einungis að vera aðgengileg innan fyrirtækisins eða stofnunar.
Engin dulkóðun.
Skjal merkt sem Innri gögn í fæti skjalsins.
Tengt DLP fyrir ytri miðlun.

Trúnaðargögn

Viðkvæm viðskiptagögn.
Dulkóðun virk fyrir takmörkun á deilingu utan fyrirtækis eða stofnunar.
Oft með undirflokkunum fyrir ytri miðlun gagna.
Tengt DLP fyrir ytri miðlun.

Afmörkuð gögn

Mjög viðkvæm gögn.
Ströng dulkóðun og aðgangsstýring.

Crayon

❌ Ekki

📋 Nota öryggisflokkun sem gátlista fyrir reglufylgni	🏷️ Nota 20+ merkingar	📝 Gleyma lýsingu á merkinguna
⏳ Láta reglur vera lengi í „hermunarham“ (Simulation mode)	🔗 Gleyma að samræma merkingar við DLP	🤝 Gleyma að taka tillit til samstarfi með ytri aðilum

Crayon

✅ Gerðu

⚠️ Áhættumat með gögnunum sem þú hefur. *„Hvaða gögn, ef þau leka, gætu skaðað okkur eða orðsporið okkar?“*

🎯 Merkingarnar einfaldar

🖍️ Stuttar en skýrar lýsingar

📊 Stöðumat á Activity explorer vikulega

🔐 Tengingu við merkingar og ákveðna DLP-aðgerðar

🌎 Prófun á deilingu með ytri aðilum

Crayon

CRAYON PURVIEW PROJECT

Planning and overview

Planning your deployment

- Define Objectives
- Assess Readiness
- Stakeholder Engagement
- Assign Roles

Purview Overview

- Data Explorer
- Data Loss Prevention
- Communication Compliance
- Data Lifecycle Management
- Auditing
- Insider Risk Management
- Data Security Posture Management
- eDiscovery

Non-IT preparation

Know your data

- What data is sensitive to your business?
- How can it be identified?

Know your risks

- Regulatory compliance
- Data exposure or leakage
- Who should (and should not) have access to this data?
- Consequences of unauthorized sharing or misuse?
- financial or reputational impact of a data breach?

Protect

Data Classification

- Define Data classification schema
- Create sensitivity labels to classify data
- Publish sensitivity labels to end-users

Data Loss Prevention

- Turn on “Analytics” to get insights in data usage
- Onboard devices to Purview
- Create DLP policy to prevent critical data from leaving the organization, without good reason
- Create DLP policy to prevent risky users from sharing data outside organization

Data Security Posture Management for AI

- Monitor AI use
- Discover and safeguard AI activity

Crayon

CRAYON PURVIEW PROJECT

Protect

Insider Risk Management

- Turn on “Analytics” to get insights in potential risks
- Turn on “Adaptive protection” to risk score users, based on behavior with data
- Enable relevant indicators to look for, when measuring insider risk
- Create data leaks policy to monitor risky behavior and risk score users
- Tune policies based on insights about user behavior, to get relevant alerts

Retention

Data Lifecycle Management

- Create Retention policies to retain or delete data according to organizational needs
- Create Retention labels to apply to specific documents

Compliance

Communication Compliance

- Develop and configure communication compliance policies
- Regularly monitor alerts generated by communication compliance policies
- Take appropriate remediation actions, such as notifying users, removing inappropriate messages, or escalating issues to relevant departments

Compliance Manager

- Use the “Data protection baseline assessment” to adhere to Microsoft best practice implementations, based on regulations such as NIST, ISO, FedRAMP, GDPR.
- Use specific assessments to adhere to specific regulations, as required by the organization

Admins

Roles and Scopes

- Create alert rule to notify when Purview roles are assigned
- Enable Purview role assignments via PIM, by assigning roles to Entra ID groups

Crayon

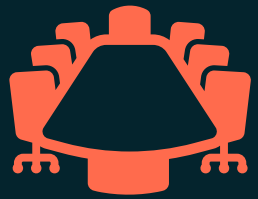
3 einföld skref

Notendaþátttaka

- Fræðsla
- Aðgangur að leiðbeiningum og stuðningi
- **Endurtaktu!**

Öryggisflokkun

- Flokkaðu gögnin
- Hafðu flokkunina einfalda
- Verndaðu gögnin



Forysta

- Stjórnendur þurfa að leiða verkefnið
- Taka ábyrgð á því hvaða gögn skipta máli

Crayon