## Αναφορά σχετικά με τις απαιτήσεις ασφάλειας δεδομένων, ασφάλειας συστήματος και GDPR

### Εισαγωγή

Ο σκοπός αυτής της έκθεσης είναι να παρουσιάσει μια επισκόπηση των απαιτήσεων Ασφάλειας Δεδομένων, Ασφάλειας Συστήματος και GDPR που σχετίζονται με το έργο του ΔΕΔΔΗΕ. Αυτή η έκθεση στοχεύει να παρέχει μια λεπτομερή ανάλυση σχετικά με τις βασικές εκτιμήσεις και τις ενέργειες που απαιτούνται για τη διατήρηση της συμμόρφωσης και τη διασφάλιση της ακεραιότητας του έργου. Η ενσωμάτωση με τις τεχνολογίες Azure θα τονιστεί για τη βελτίωση αυτών των απαιτήσεων.

### Απαιτήσεις ασφάλειας δεδομένων

Η ασφάλεια των δεδομένων είναι πρωταρχικής σημασίας για την προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις και άλλες απειλές. Ακολουθούν οι κρίσιμες απαιτήσεις για την ασφάλεια των δεδομένων και πώς μπορούν να ενσωματωθούν οι τεχνολογίες Azure:

#### 1. Κρυπτογράφηση δεδομένων

* Κρυπτογράφηση σε κατάσταση ηρεμίας και κατά τη μεταφορά: Εφαρμογή μεθόδων κρυπτογράφησης όπως το AES-256 για την προστασία των δεδομένων που είναι αποθηκευμένα σε μονάδες δίσκου (σε κατάσταση ηρεμίας) και κατά τη μετάδοση μέσω δικτύων (σε μεταφορά).
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε την κρυπτογράφηση υπηρεσίας αποθήκευσης Azure (SSE) για δεδομένα σε κατάσταση ηρεμίας και την κρυπτογράφηση εικονικού δικτύου Azure για δεδομένα υπό μεταφορά.
  + Βιβλιογραφικές αναφορές:
    - [Κρυπτογράφηση υπηρεσίας αποθήκευσης Azure](https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption)
    - [Κρυπτογράφηση εικονικού δικτύου Azure](https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview)

#### 2. Έλεγχος πρόσβασης

* **Έλεγχος πρόσβασης βάσει ρόλων (RBAC)** : Καθορισμός και επιβολή ρόλων και αδειών χρήστη για περιορισμό της πρόσβασης σε δεδομένα με βάση την αρχή του ελάχιστου προνομίου.
  + **Ενσωμάτωση Azure** : Εφαρμόστε το Azure RBAC για να διαχειριστείτε ποιος έχει πρόσβαση στους πόρους του Azure.
  + Βιβλιογραφικές αναφορές:
    - [Έλεγχος πρόσβασης βάσει ρόλων Azure](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)
* **Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)** : Εφαρμογή MFA για την προσθήκη ενός επιπλέον επιπέδου ασφάλειας για την πρόσβαση σε ευαίσθητα δεδομένα, διασφαλίζοντας ότι οι χρήστες επαληθεύονται με πολλαπλές μεθόδους.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων Azure.
  + Βιβλιογραφικές αναφορές:
    - [Azure Multi- Factor Authentication](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted)

#### 3. Προστασία Δεδομένων

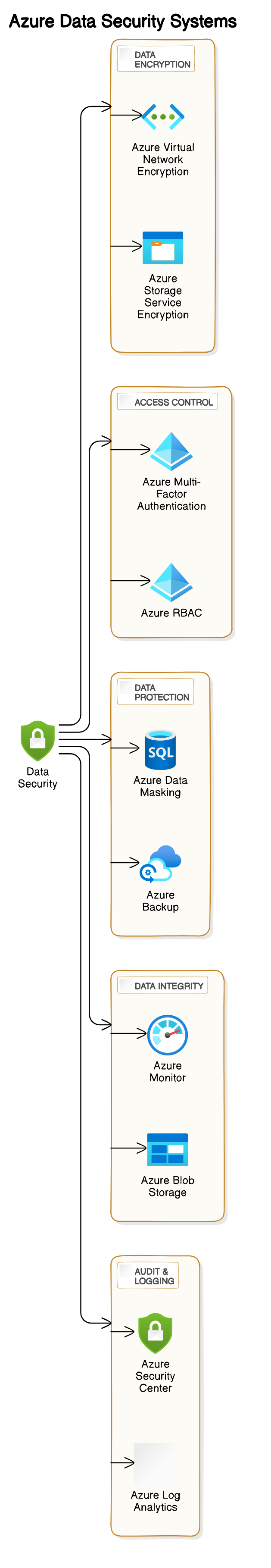
* **Τακτικά αντίγραφα ασφαλείας** : Διεξαγωγή συχνών αντιγράφων ασφαλείας δεδομένων και αποθήκευση τους με ασφάλεια για την αποφυγή απώλειας δεδομένων σε περίπτωση αστοχιών του συστήματος ή συμβάντων στον κυβερνοχώρο.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Backup για αξιόπιστα και ασφαλή αντίγραφα ασφαλείας.
  + Βιβλιογραφικές αναφορές:
    - [Azure Backup](https://docs.microsoft.com/en-us/azure/backup/backup-overview)
* **Απόκρυψη και ανωνυμοποίηση δεδομένων** : Χρήση τεχνικών για την ανωνυμοποίηση και απόκρυψη ευαίσθητων δεδομένων, μειώνοντας τον κίνδυνο έκθεσης κατά την επεξεργασία και ανάλυση δεδομένων.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε τη δυναμική κάλυψη δεδομένων βάσης δεδομένων Azure SQL και την ανάλυση Azure Data Lake για ανωνυμοποίηση.
  + Βιβλιογραφικές αναφορές:
    - [Δυναμική κάλυψη δεδομένων βάσης δεδομένων Azure SQL](https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview)
    - [Azure Data Lake Analytics](https://docs.microsoft.com/en-us/azure/data-lake-analytics/data-lake-analytics-overview)

#### 4. Ακεραιότητα δεδομένων

* **Έλεγχοι ακεραιότητας** : Χρησιμοποιώντας αθροίσματα ελέγχου και κατακερματισμούς για την επαλήθευση της ακεραιότητας των δεδομένων, διασφαλίζοντας ότι παραμένουν αμετάβλητα και αμετάβλητα.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Blob Storage που υποστηρίζει κατακερματισμό MD5 για ακεραιότητα δεδομένων.
  + Βιβλιογραφικές αναφορές:
    - [Κατακερματισμός Azure Blob Storage MD5](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-md5-checksum)
* **Πρόληψη μη εξουσιοδοτημένων τροποποιήσεων** : Εφαρμογή μηχανισμών για τον εντοπισμό και την πρόληψη μη εξουσιοδοτημένων τροποποιήσεων δεδομένων.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε την οθόνη Azure για να εντοπίσετε μη εξουσιοδοτημένες τροποποιήσεις.
  + Βιβλιογραφικές αναφορές:
    - [Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/overview)

#### 5. Έλεγχος και Καταγραφή

* **Ολοκληρωμένη καταγραφή** : Διατήρηση λεπτομερών αρχείων καταγραφής πρόσβασης δεδομένων, τροποποιήσεων και μεταφορών για τη διευκόλυνση του ελέγχου και της εγκληματολογικής ανάλυσης.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Log Analytics για λεπτομερή καταγραφή.
  + Βιβλιογραφικές αναφορές:
    - [Azure Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview)
* **Τακτικοί έλεγχοι** : Διενέργεια τακτικών ελέγχων για τη διασφάλιση της τήρησης των πολιτικών ασφάλειας δεδομένων και τον εντοπισμό πιθανών τρωτών σημείων.
  + **Azure Integration** : Χρησιμοποιήστε το Azure Security Center για συνεχή αξιολόγηση ασφάλειας.
  + Βιβλιογραφικές αναφορές:
    - [Κέντρο Ασφαλείας Azure](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro)
* Ασφάλεια δεδομένων Azure



### Απαιτήσεις ασφάλειας συστήματος

Η ασφάλεια του συστήματος περιλαμβάνει μέτρα για την προστασία της υποδομής του δικτύου, του υλικού και του λογισμικού από απειλές και τρωτά σημεία. Οι βασικές απαιτήσεις περιλαμβάνουν:

#### 1. Ασφάλεια Δικτύου

* **Τείχη προστασίας και IDS/IPS** : Ανάπτυξη τειχών προστασίας και συστημάτων ανίχνευσης/αποτροπής εισβολής για την παρακολούθηση και τον έλεγχο της εισερχόμενης και εξερχόμενης κίνησης δικτύου με βάση προκαθορισμένους κανόνες ασφαλείας.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το τείχος προστασίας Azure και την προστασία Azure DDoS.
  + Βιβλιογραφικές αναφορές:
    - [Τείχος προστασίας Azure](https://docs.microsoft.com/en-us/azure/firewall/overview)
    - [Προστασία Azure DDoS](https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview)
* **Secure Network Architecture** : Σχεδιασμός μιας ασφαλούς αρχιτεκτονικής δικτύου με τμηματοποίηση για την απομόνωση κρίσιμων συστημάτων και δεδομένων από πιθανές απειλές.
  + **Ενοποίηση Azure** : Χρησιμοποιήστε το εικονικό δίκτυο Azure για να δημιουργήσετε μεμονωμένα τμήματα δικτύου.
  + Βιβλιογραφικές αναφορές:
    - [Εικονικό δίκτυο Azure](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview)

#### 2. Ασφάλεια τελικού σημείου

* **Antivirus και Anti-Malware** : Εγκατάσταση και τακτική ενημέρωση λογισμικού προστασίας από ιούς και κακόβουλου λογισμικού για την προστασία των τελικών σημείων από κακόβουλες επιθέσεις.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Microsoft Defender για Endpoint.
  + Βιβλιογραφικές αναφορές:
    - [Microsoft Defender για Endpoint](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint)
* **Επιδιορθώσεις συστήματος και ενημερώσεις** : Διασφάλιση ότι όλα τα συστήματα και το λογισμικό επιδιορθώνονται και ενημερώνονται τακτικά για τον μετριασμό των τρωτών σημείων.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε τη Διαχείριση Ενημερώσεων Αυτοματισμού Azure.
  + Βιβλιογραφικές αναφορές:
    - [Διαχείριση ενημέρωσης αυτοματισμού Azure](https://docs.microsoft.com/en-us/azure/automation/automation-update-management)

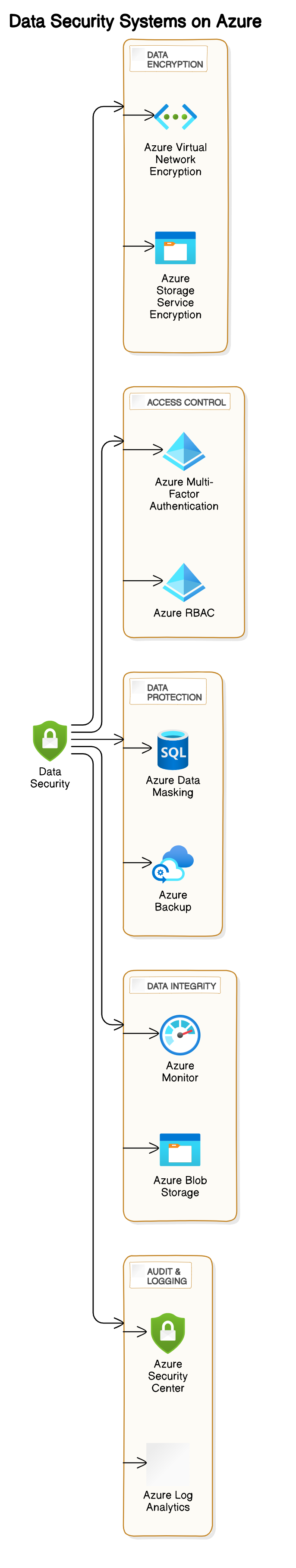
#### 3. Φυσική Ασφάλεια

* **Έλεγχοι πρόσβασης** : Εφαρμογή φυσικών ελέγχων πρόσβασης σε κέντρα δεδομένων και διακομιστές, συμπεριλαμβανομένων βιομετρικών σαρωτών και συστημάτων καρτών-κλειδιών.
  + **Ενσωμάτωση Azure** : Τα κέντρα δεδομένων Azure ακολουθούν αυστηρά πρωτόκολλα φυσικής ασφάλειας.
  + Βιβλιογραφικές αναφορές:
    - [Φυσική ασφάλεια Azure Datacenter](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security)
* **Επιτήρηση και παρακολούθηση** : Χρήση καμερών παρακολούθησης και συστημάτων παρακολούθησης για την ασφάλεια φυσικών τοποθεσιών και τον εντοπισμό μη εξουσιοδοτημένης πρόσβασης.
  + **Ενσωμάτωση Azure** : Τα κέντρα δεδομένων Azure είναι εξοπλισμένα με συστήματα επιτήρησης.
  + Βιβλιογραφικές αναφορές:
    - [Azure Datacenter Surveillance](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security)

#### 4. Ασφάλεια Εφαρμογών

* **Πρακτικές Ασφαλούς Ανάπτυξης** : Υιοθέτηση προτύπων ασφαλούς κωδικοποίησης, διεξαγωγή ελέγχων κώδικα και εφαρμογή δοκιμών ασφαλείας σε όλο τον κύκλο ζωής ανάπτυξης λογισμικού.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure DevOps για ασφαλείς αγωγούς CI/CD.
  + Βιβλιογραφικές αναφορές:
    - [Azure DevOps](https://docs.microsoft.com/en-us/azure/devops/?view=azure-devops)
* **Εκτιμήσεις ευπάθειας** : Διεξαγωγή τακτικών αξιολογήσεων ευπάθειας και δοκιμών διείσδυσης για τον εντοπισμό και την αποκατάσταση αδυναμιών ασφάλειας.
  + **Azure Integration** : Χρησιμοποιήστε το Azure Security Center για αξιολογήσεις ευπάθειας.
  + Βιβλιογραφικές αναφορές:
    - [Κέντρο Ασφαλείας Azure](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro)

#### 5. Αντιμετώπιση περιστατικού

* **Σχέδιο Αντιμετώπισης Συμβάντων** : Ανάπτυξη και διατήρηση ενός ολοκληρωμένου σχεδίου αντιμετώπισης συμβάντων για την αποτελεσματική αντιμετώπιση και άμβλυνση περιστατικών ασφαλείας.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Sentinel για ανίχνευση και απόκριση περιστατικού.
  + Βιβλιογραφικές αναφορές:
    - [Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/overview)
* **Εκπαίδευση και ασκήσεις** : Διεξαγωγή τακτικών εκπαιδευτικών συνεδριών και ασκήσεων για την ομάδα αντιμετώπισης περιστατικών για να διασφαλιστεί η ετοιμότητα για πιθανές παραβιάσεις της ασφάλειας.
  + **Azure Integration** : Αξιοποιήστε τους πόρους εκπαίδευσης της Microsoft για την απόκριση σε περιστατικά.
  + Βιβλιογραφικές αναφορές:
    - [Microsoft Training](https://docs.microsoft.com/en-us/learn/)
* **Ασφάλεια συστήματος Azure**
* 

### Απαιτήσεις GDPR

Η συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) είναι απαραίτητη για την προστασία των προσωπικών δεδομένων και τη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων. Οι βασικές απαιτήσεις GDPR περιλαμβάνουν:

#### 1. Δικαιώματα υποκειμένου δεδομένων

* **Αιτήματα πρόσβασης** : Εφαρμογή μηχανισμών για τη διαχείριση αιτημάτων πρόσβασης υποκειμένων δεδομένων (DSAR), που επιτρέπουν στα άτομα να έχουν πρόσβαση στα προσωπικά τους δεδομένα.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Active Directory για να διαχειριστείτε αιτήματα πρόσβασης.
  + Βιβλιογραφικές αναφορές:
    - [Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis)
* **Διόρθωση, διαγραφή και περιορισμός** : Παροχή διαδικασιών για τα υποκείμενα των δεδομένων για διόρθωση, διαγραφή ή περιορισμό της επεξεργασίας των προσωπικών τους δεδομένων.
  + **Azure Integration** : Χρησιμοποιήστε το Azure Data Factory για να αυτοματοποιήσετε τις διαδικασίες διαχείρισης δεδομένων.
  + Βιβλιογραφικές αναφορές:
    - [Azure Data Factory](https://docs.microsoft.com/en-us/azure/data-factory/)

#### 2. Διαχείριση συναίνεσης

* **Λήψη συγκατάθεσης** : Διασφάλιση ότι η συγκατάθεση λαμβάνεται από τα υποκείμενα των δεδομένων με σαφή και διαφανή τρόπο, με δυνατότητα εύκολης ανάκλησης της συγκατάθεσης.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε την Πολιτική Azure για να επιβάλετε τη συμμόρφωση με τη διαχείριση συναίνεσης.
  + Βιβλιογραφικές αναφορές:
    - [Πολιτική Azure](https://docs.microsoft.com/en-us/azure/governance/policy/overview)
* **Σημειώσεις απορρήτου** : Παροχή σαφών και προσβάσιμων ειδοποιήσεων απορρήτου που ενημερώνουν τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων.
* **Ενσωμάτωση Azure** : Χρησιμοποιήστε την Προστασία πληροφοριών Azure για την επισήμανση και την προστασία των εγγράφων.
* Βιβλιογραφικές αναφορές:
  + [Προστασία πληροφοριών Azure](https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection)

#### 3. Ειδοποίηση παραβίασης δεδομένων

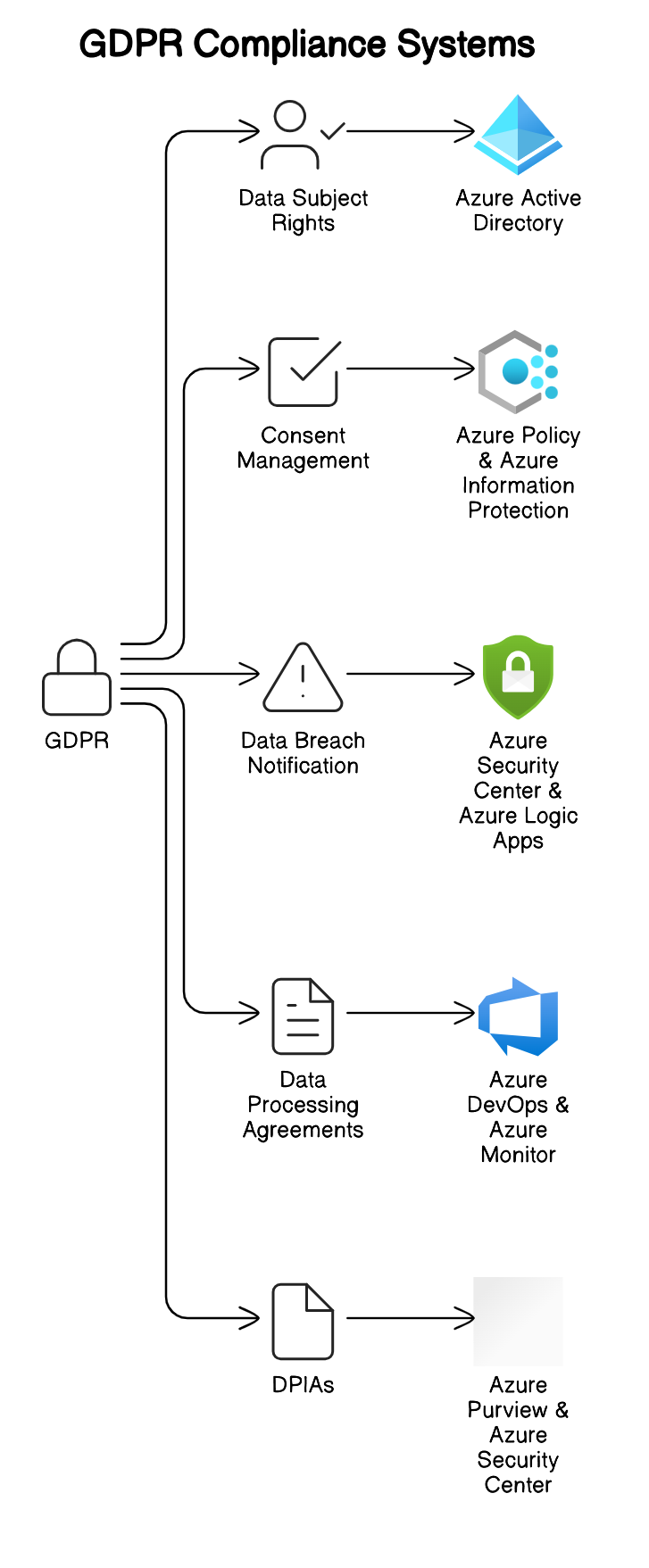
* **Ανίχνευση και αναφορά** : Εφαρμογή διαδικασιών για τον έγκαιρο εντοπισμό, αναφορά και διερεύνηση παραβιάσεων δεδομένων.
  + **Azure Integration** : Χρησιμοποιήστε το Azure Security Center για ανίχνευση απειλών σε πραγματικό χρόνο.
  + Βιβλιογραφικές αναφορές:
    - [Κέντρο Ασφαλείας Azure](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro)
* **Απαιτήσεις ειδοποίησης** : Διασφάλιση ότι οι παραβιάσεις δεδομένων αναφέρονται στις αρμόδιες αρχές και τα επηρεαζόμενα άτομα εντός 72 ωρών.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε τις εφαρμογές Azure Logic για να αυτοματοποιήσετε τις ροές εργασίας ειδοποιήσεων παραβίασης.
  + Βιβλιογραφικές αναφορές:
    - [Εφαρμογές Azure Logic](https://docs.microsoft.com/en-us/azure/logic-apps/)

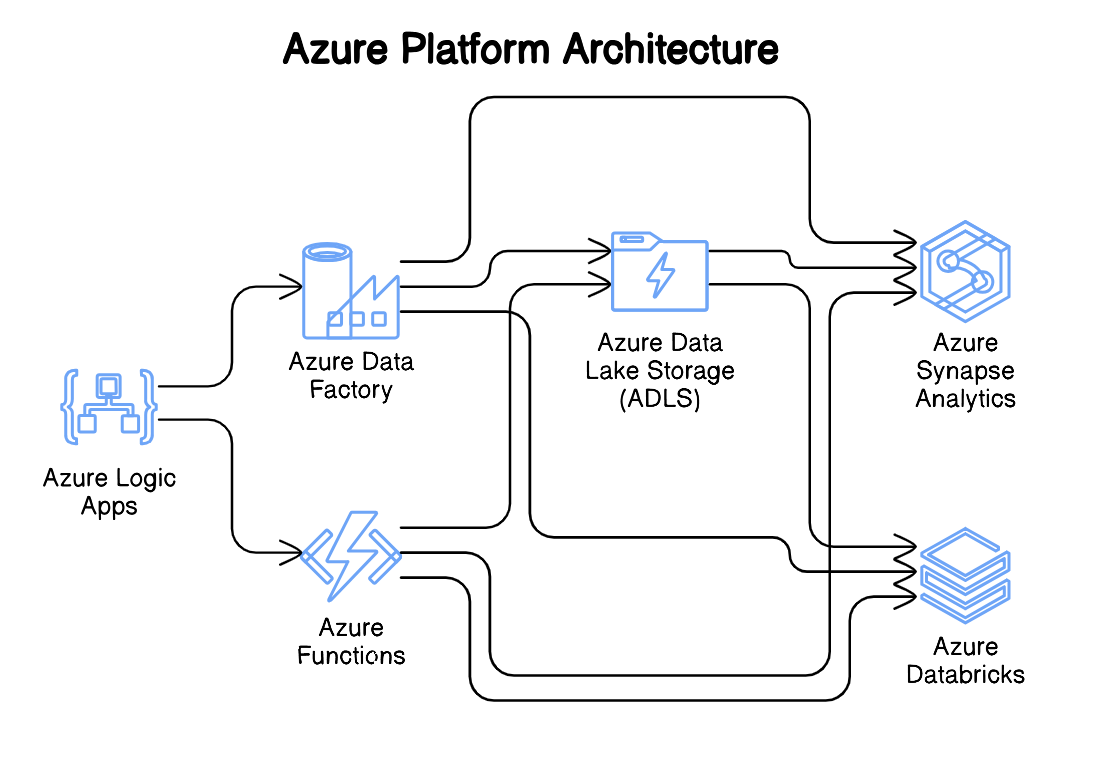
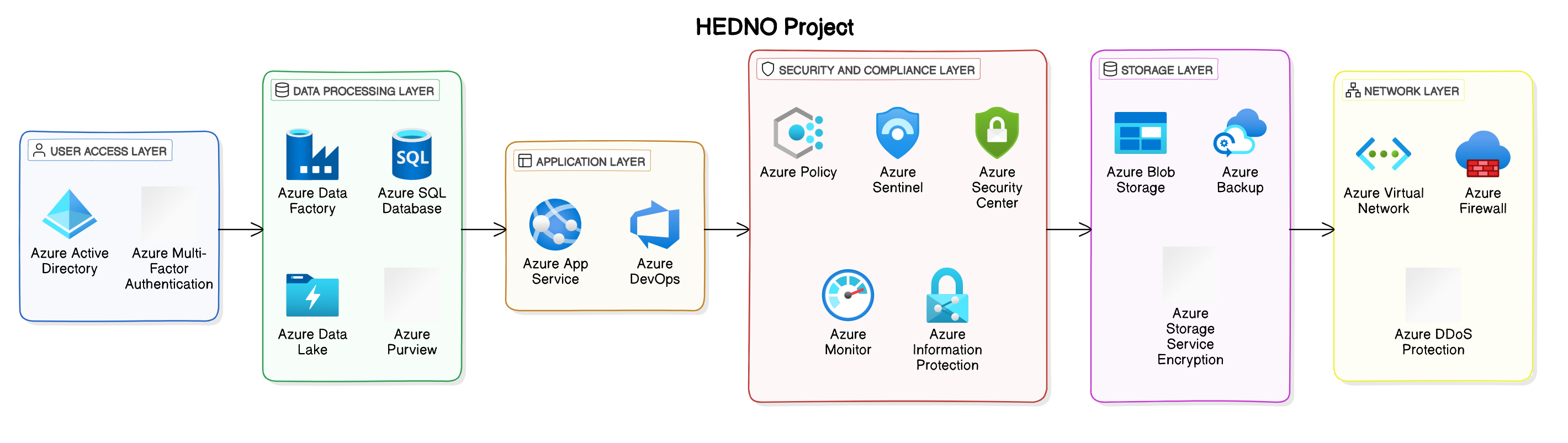
#### 4. Συμφωνίες Επεξεργασίας Δεδομένων

* **Συμμόρφωση τρίτων μερών** : Σύναψη συμφωνιών επεξεργασίας δεδομένων με όλους τους τρίτους φορείς επεξεργασίας για τη διασφάλιση της συμμόρφωσης με τον GDPR.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure DevOps για να διαχειριστείτε τις συμβάσεις και την τεκμηρίωση συμμόρφωσης.
  + Βιβλιογραφικές αναφορές:
    - [Azure DevOps](https://docs.microsoft.com/en-us/azure/devops/?view=azure-devops)
* **Τακτικές αναθεωρήσεις** : Διενέργεια τακτικών επιθεωρήσεων και ελέγχων τρίτων επεξεργαστών για τη διασφάλιση της συνεχούς συμμόρφωσης.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Monitor για να παρακολουθείτε μετρήσεις συμμόρφωσης.
  + Βιβλιογραφικές αναφορές:
    - [Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/overview)

#### 5. Εκτιμήσεις Επιπτώσεων Προστασίας Δεδομένων (ΕΑΠΔ)

* **Διενέργεια ΕΑΠΔ** : Διεξαγωγή ΕΑΠ για δραστηριότητες επεξεργασίας που ενέχουν υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Purview για διαχείριση και αξιολόγηση δεδομένων.
  + Βιβλιογραφικές αναφορές:
    - [Azure Purview](https://docs.microsoft.com/en-us/azure/purview/)
* **Μετριασμός κινδύνου** : Εντοπισμός και μετριασμός κινδύνων που σχετίζονται με δραστηριότητες επεξεργασίας δεδομένων για τη διασφάλιση της συμμόρφωσης με τον GDPR.
  + **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Security Center για να εντοπίσετε και να μειώσετε τους κινδύνους.
  + Βιβλιογραφικές αναφορές:
    - [Κέντρο Ασφαλείας Azure](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro)
  + **Azure GDPR**



* **Γενική Αρχιτεκτονική Επισκόπηση**  
  
* **Ειδική Επισκόπηση έργου**  
  

### συμπέρασμα

Αυτή η έκθεση περιγράφει τις βασικές απαιτήσεις Ασφάλειας Δεδομένων, Ασφάλειας Συστήματος και GDPR που σχετίζονται με το έργο του ΔΕΔΔΗΕ. Η ενσωμάτωση με τις τεχνολογίες Azure παρέχει ισχυρές λύσεις για την κάλυψη αυτών των απαιτήσεων, διασφαλίζοντας ότι το έργο διατηρεί τα υψηλότερα πρότυπα ασφάλειας και συμμόρφωσης.

Η ομάδα Incelligent θα πρέπει να επανεξετάσει και να διασφαλίσει ότι όλα τα καθορισμένα μέτρα εφαρμόζονται και διατηρούνται καθ' όλη τη διάρκεια του κύκλου ζωής του έργου για την τήρηση των υψηλότερων προτύπων ασφάλειας και συμμόρφωσης. Εάν χρειάζονται περαιτέρω λεπτομέρειες ή διευκρινίσεις, ανατρέξτε στα σχετικά αρχεία ή επικοινωνήστε με τους σχετικούς ενδιαφερόμενους φορείς.

### Σχετικά Αρχεία κατά Απαίτηση

A screenshot of a computer

Description automatically generated