Private by design Android apps

https://d.android.com/design-for-safety

Requesting runtime permissions

- Declare permissions
- Increase educational content & wait for user action
- Check for permission
- Show dialog if required
- Request permission
- Handle response
- Creatively degrade experience (Do Action)

Permission minimized requests

registerForActivityResult(ActivityResultCallback()) { w1l -> _ }

Permission denied

If the user deny a permission, gracefully degrade your app experience

- Clearly highlight the features / part of your app with limited functionality due to the permission denial
- Let users continue to use other features in your app normally

Security

- Protect user data
- Ensure integrity
- Ensure availability

Use photo picker

Use Photo Picker to provide a seamless and permissionless user experience to select visual media file and simplify developer costs

Understanding where and how your app is accessing user data

Use data access audit XMLs to gain insights into how your app & its dependencies (including SDKs & 3rd party libraries) access private data from users

Set up callback to log different forms of data access

val appOpsManager = getPackageManager().getAppOpsManager()
val privacyIngressProfile = appOpsManager.getPrivacyIngressProfile()

Data Safety Labels

- The Data Safety section on Google Play specifies the user data your app collects or shares
- Fill out the form in Play Console (Privacy + App content) based on your app and 3rd party SSM data usage
- Info from your app will be highlighted in your app’s Play Store page and for certain critical app permission requests

Location minimization

- Always request ACCESS_COARSE_LOCATION only first
- Ensure your app still works if a user grants coarse access only
- Reduce location computation by choosing the best location estimate
- Use FusedLocationProvider to ensure correct access form factors (e.g. tablets)

Optional location minimization

Only a few core services allowed (such as geofencing)

Before requesting, user must grant fine &/or coarse permissions first

Requires ACCESS_BACKGROUND_LOCATION permission

Location frequency might be affected by background location limits

Android 11

- Stoped storage enhancements
- Separate secure for background location
- Data access auditing

Android 12

- Appropriate location
- Privacy dashboard
- Bluetooth permissions

Android 13

- Selected media access
- Data safety in permissions
- Screenshot deletion

Android 14

Choose the right storage

- App-specific storage
- Shared storage
- Preference
- Databases

Last update: 13 March 2019